SEE FOLLOWING NOTE

PARTS OF THE ORIGINAL DOCUMENT

ARE OF POOR REPRODUCTIVE QUALITY

CERTAINES PARTIES DU DOCUMENT ORIGINAL

SONT DE PIÈTRE QUALITÉ DE REPRODUCTION

Annual Report
Privacy Commissioner
1987-88

The Privacy Commissioner of Canada
112 Kent Street
Ottawa, Ontario
K1A 1H3
(613) 995-2410, 1-800-267-0441

The switchboard is open from 7:30 a.m. to 6:00 p.m., Ottawa time.

© Minister of Supply and Services Canada 1988

Cat. No. IP30-1/1988

ISBN 0-662-55287-3

"No personal information shall be collected . . . unless it relates directly to an operating program or activity . . . ".

"A government institution shall, wherever possible, collect personal information . . . directly from the individual to whom it relates . . .

". . . shall inform any individual . . . of the purpose for which the information is being collected.

". . . shall take all reasonable steps to ensure that personal information . . . is as accurate, up-to-date and complete as possible.

"Personal information . . . shall not, without the consent of the individual to whom it relates, be used . . . except

(a) for the purpose for which the information was obtained or compiled . . ."

(or in accordance with specific exceptions set out in section 8)

The *Privacy Act*

The Honourable Guy Charbonneau
The Speaker
The Senate
Ottawa

June 30, 1988

Dear Mr. Charbonneau:

I have the honour to submit to Parliament my annual report. This report covers the period from April 1, 1987, to March 31, 1988.

Yours sincerely,

John W. Grace

John W. Grace
Privacy Commissioner

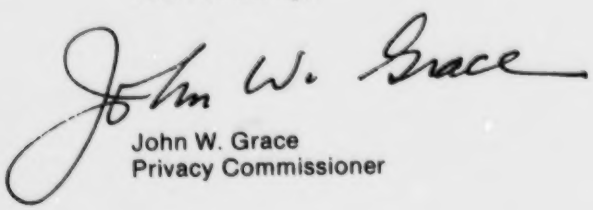
The Honourable John Fraser, P.C., Q.C., M.P.
The Speaker
The House of Commons
Ottawa

June 30, 1988

Dear Mr. Fraser:

I have the honour to submit to Parliament my annual report. This report covers the period from April 1, 1987, to March 31, 1988.

Yours sincerely,



John W. Grace
Privacy Commissioner

Contents

Mandate 1

Five Years in a Life 2

Issues - Old and New 14
- Data Matching and SIN 14
- "Consistent Use" 15
- Parolees, Inmates and Privacy 16
- Privacy in the Workplace 18

Complaints Branch 22
- Complaints 23
- Using the Privacy Act 37

Compliance Branch 38
- The Audits 39
  - Environment Canada 39
  - Transport Canada 40
  - Agriculture Canada 42
  - Correctional Service Canada 43

Notifying the Commissioner 44

Spreading the Word 45

Inquiries 46

Corporate Management 47

Appendices
- I Organization Chart 49
- II Government Institutions Covered by the Act 50

Mandate

The *Privacy Act* provides individuals with access to their personal information held by the federal government; it protects individuals' privacy by limiting those who may see the information; and it gives individuals some control over the government's collection and use of the information.

The Act sets out the principles of fair information practices, requiring government to:

- collect only the information needed to operate its programs;
- collect the information directly from the individual concerned, whenever possible; and
- tell the individual how it will be used;
- keep the information long enough to ensure an individual access; and
- "take all reasonable steps" to ensure its accuracy and completeness

Canadian citizens or permanent residents may complain to the Privacy Commissioner if:

- they are denied any part of the information;
- they are denied their request to correct some of the information on the file — or their right to annotate it;
- the department takes longer than the initial 30 days or maximum 60 days to provide the information;
- the Personal Information Index description of the contents of the information bank is deficient in some way;
- the department's listing in the Index does not describe all the uses it makes of personal information;
- an institution is collecting, keeping or disposing of personal information in a way which contravenes the *Privacy Act*.

The Privacy Commissioner's investigators examine any file (including those in closed banks) except confidences of the Queen's Privy Council to ensure that government institutions are complying with the Act.

The Act also gives the Privacy Commissioner the power to audit the way government institutions are collecting, using and disposing of personal information, without having to wait for a complaint.

Five Years in a Life

It is now five years of life under the *Privacy Act*, five years of these accountings to Parliament (and the country) on how its legislation is being observed; five years of alarums and preachments over the threats of the new information technologies — usually in their benign guise of efficiency — to precious and vulnerable human values.

Not a long span in the life of a law. Not a long time to show results within a system as multifarious and intractable as the federal government establishment. Yet the conclusion in this fifth year must be that the *Privacy Act* has already proved its value beyond all the early (and often understandable) skepticism. That judgment is not of a privacy partisan such as the Privacy Commissioner but of the government as it responded this past year to the remarkably comprehensive and highly supportive review of the Act by a committee of Parliament.

The issue at this five-year point is not the need for privacy legislation, but whether its sweep and its powers are sufficient for the threat and the challenge.

It is hardly conceivable today that a democratic country would not control the use of personal information which its government collects from individuals in ever-increasing amounts. The new privacy threats are so explosive, so unexpected that a single code probably cannot be written to cover them.

Consider what happened to Robert Bork in the midst of the Senate hearings into his nomination as a Justice of the United States Supreme Court. A Washington newspaper obtained and published a list of the movies that Mr. Bork had rented from a video store. But until this outrageous invasion of personal privacy had occurred, who had worried about protecting the privacy of video store customers? (One U.S. senator was so appalled by the lapse of journalistic standards that he brought copies of his own video records to the committee to show how they can be misconstrued. His list revealed that he had rented something the store called "Cat on a Hot" which was the short form for "Cat on a Hot Tin Roof".)

As the direct result of the abuse of Mr. Bork's privacy, legislation has been proposed in some American states to bar such a repellent practice.

But what will the next law be required to stop? Where will the next scary breach of privacy come from? Are we to worry about public libraries releasing lists of their borrowers' selections to investigators or journalists? Pray not! But record-keepers, be they in a video store, a library, personnel or credit card office, can spill out at the push of a button personal information to damage, to defame or merely to titillate.

Another example of the difficulty of keeping privacy protection ahead of technology (and, sometimes, hysteria) is found in the proliferation of tests of greater or lesser reliability.

Old-fashioned, personal evaluations of suitability, character and experience are giving way to science and psuedo-science. One American privacy specialist, Robert Ellis Smith, has observed that in his country it is becoming commonplace for employees to face fingerprinting, lie detectors, urinalysis, psychological tests, blood tests, computerized criminal record checks, handwriting analysis and, yes, clearance by astrology.

In the *New York Times,* William Safire wrote:

> "We are frisking each other. Picture yourself going to work tomorrow, handing over blood and urine samples, taking a quick turn with the house polygraph, turning out your pockets and walking through some new fluoroscope. You object? Whatsamatter, you got something to hide?"

Nothing at all to hide; privacy and dignity to lose.

John Shattuck, who teaches privacy law at Harvard and is a vice-president of that university, has said that there is "a basic unregulated quality" to the new systems and practices which invade the sanctuaries of what once were private places. The new technologies are outside the traditional boundaries of privacy law, Mr. Shattuck says, "either because there is no law, because the law is obsolete, or because a decision has been made simply not to apply the law".

Not a situation to please anyone, liberal or conservative, left wing or right.

The use of the so-called objective and impersonal tests becoming routine in some places is not yet out of control in Canada but, unless care is taken, we may be seeing our future elsewhere.

Protection Improves

Comfort should be taken where it can be found. It can be said that after five years Canada's *Privacy Act* continues to be applied with increasing sensitivity and rigor. While the application remains uneven, there can be growing, not shrinking, confidence that information which individuals give their federal government — often with no choice — will be used only for the purposes for which it is given and will be seen only by persons with the need or right to know.

These are important principles to defend and enforce. Those who know use their knowledge, a truism, as *The Economist* has observed, applying "to many down the years, from tempted Eve in the Garden of Eden to Ivan Boesky in New York" or, bringing the matter closer to home, to a cabinet minister in Nova Scotia.

Privacy laws exist first of all to protect people. Legislators have brought them forward out of the most benevolent of motives: the conviction that their constituents need to be defended from the misuse of their personal information by the state.

But governments should recognize that they too become beneficiaries of effective data protection, though on occasion it may be a nuisance or an embarrassment. Individuals will be more likely to give their government

better quality information, whether required by law as in a census or in tax returns, or in a voluntary survey, if they know that such personal information is protected by the principles found in the *Privacy Act.*

Moreover, countries with data protection laws are showing an increasing reluctance to allow their citizens' data to flow unrestrained to countries without such laws. Off-shore "data havens" would pose sovereignty and economic as well as privacy threats.

It is not entirely pure benevolence, therefore, that this past year has motivated such diverse countries as the Netherlands, Greece, Ireland, Finland and Japan to bring forward privacy legislation broadly similar to that which has been in place in Canada's *Privacy Act* for five years (three years earlier counting Part IV of the *Canadian Human Rights Act*).

Whatever the motives, the enhancement of privacy protection is on some national agendas, far perhaps from the top, but at least under "other matters".

The good privacy news in Canada last year, the biggest news in the privacy business, was not — let us be grateful — of new privacy Chernobyls, or even of more extravagantly lost documents; that epidemic has apparently passed. No, the central event — entirely reassuring — was the government's commitment to the acceptance of key recommendations of *Open and Shut: Enhancing the Right to Know and the Right to Privacy,* the report of the Committee on Justice and Solicitor General after its review of the *Privacy Act* and the *Access to Information Act.*

> "The government agrees that changes can be made to the *Privacy Act* to make it more effective as a data-protection statute. This will allow it to remain on the cutting-edge for matters concerning protection of personal information and the setting of standards for effective controls on the collection, use and disclosure of such information by government institutions."

There it was; a Privacy Commissioner could not have put it better. The words are from the government's policy paper, *The Steps Ahead,* issued in response to the committee's recommendations.

Change Is On

Best of all, the game's afoot: significant changes have begun, none more important than the new data-matching policy being put in place. The new policy gives Canada what may well be the toughest and, from a privacy protector's point of view, the most enlightened data-matching code anywhere in the world.

Five years ago, the term "computer-matching" or "data-matching", if heard at all, was probably associated with some high-tech, lonely-hearts introduction service. In fact it is a technique which, unbridled, would present an Orwellian threat which even Orwell could not have imagined. The invasive, indiscriminate use of the computer in gathering, storing and comparing personal information for purposes either benign or malign, reduces individuals to commodities, subjugates human values to mere efficiency.

It would be foolish and dangerous to claim that the genie has been pushed all the way back into the bottle. But the new data-matching policy, effectively applied, makes it possible to entertain reasonable hope that the age of the transparent citizen can at least be delayed.

Perhaps it is neo-Luddite and unrealistic to argue that under no circumstances should data-matching be allowed. The benefits of the computer are not to be denied. The issue, cited four years ago in the Privacy Commissioner's report, is "the adequacy of safeguards to prevent violations of personal privacy". The notion was expressed that data-matching which uses an individual's personal information without knowledge and consent for purposes other than for which it was given was at least implicitly prohibited by the *Privacy Act*.

It was reassuring to have in *The Steps Ahead* the government's view that "the current *Privacy Act* provides sufficient authority to regulate data-matching and data linkage". The question then is one of the effectiveness of the regulation.

This can be said: if the new data-matching and linkage policy is observed in letter and spirit, Canadians for the first time have a reasonable assurance that their privacy will not be systematically breached as the custodians of enormous federal government data banks allow their whirring computers to run free. In fact, the gleam has been taken out of the eyes of some data processors.

Even if the *Privacy Act* had accomplished nothing else in the past year — or the past five years — it has justified its existence by being the instrument of control over data-matching. The significance of the accomplishment cannot be over-stated.

Two years ago, Professor Kenneth C. Laudon, an American authority on computer systems, wrote a book called *Dossier Society*, such a society being the dark side of the information economy. The strength of the new technology lies, Professor Laudon observes, "in its ability to move data efficiently across organizational boundaries and combine it with data from entirely different programs and files".

Here is Professor Laudon's description of the most significant characteristic of the "dossier society" from the individual's point of view:

> "...decisions made about us as citizens, employees, consumers, debtors and supplicants rely less and less on personal face-to-face contact, on what we say or even what we do. Instead, decisions are based on information that is held in national systems, and interpreted by bureaucrats and clerical workers in distant locations ... decisions based on a comprehensive 'data image' drawn from diverse files."

The *Privacy Act* is the only mechanism Canada has standing in the way of unchecked federal government surveillance by computer. And, as has been acknowledged in previous reports, the justification for information sharing, so far, has been unfailingly good — tracking down those who refuse to pay court-ordered support to children and former spouses, catching welfare cheats and debtors, establishing centralized police information systems.

It is precisely the goodness of the cause which makes matching both so attractive and so hard to stop. Yet, Professor Laudon maintains that unrestrained matching bestows upon a central government an "aggregation of power" over its citizens without precedent in peacetime and without constitutional consent. Whenever bureaucrats meet to design national information systems, it is Professor Laudon's startling conclusion that "a small constitutional convention is in progress". Though this may be an exaggeration, the consequences for computer centralization and sharing of personal information on a national scale could be much more serious than generally realized in this country.

That is why the federal government's commitment to control its own computers, using the authority of the *Privacy Act*, is the best privacy news of the year — or many years. The challenge now for the Privacy Commissioner's office is to monitor the policy effectively. The dawning of the age of the dossier society need not be upon us.

Saying no to SIN

The year produced additional encouraging privacy news as the government formally acknowledged that Canadians do not want the Social Insurance Number (SIN) to become a universal identifier. *The Steps Ahead* makes the commitment, so far as the federal government is concerned, that "no right, benefit or privilege will be withheld from and no penalty be imposed on" any individual who refuses to disclose his or her SIN except where its provision is required by law.

That policy falls short of the recommendation, made in this report last year, that no organization, government or otherwise, should be able to deny goods, services or benefits for failure to produce a SIN — unless, of course, it was specifically demanded by statute. Yet a good start has been made. The legal obstacles to launching a broader attack on the tyranny of the SIN are undoubtedly formidable.

Even so, the iron fist is almost showing through the velvet glove. The government has said that if the public sector and the private sector do not bring the use of SIN under control "legislative alternatives" will be explored "including, if necessary, an amendment to the Criminal Code to prohibit a request for the number unless authorized by law".

In setting forth tough controls against the proliferation of abuses of the SIN within its own establishment, the government puts itself in a much stronger moral position to preach on the wages of SIN both to other public jurisdictions and the private sector.

On To Crown Corps

The third piece of good news in the privacy year was the promise to extend the mandate of the *Privacy Act* to cover federal Crown corporations and their wholly-owned subsidiaries. This was the recommendation of the parliamentary review committee. The government did not accept the committee's much broader recommendation that the federally-regulated private sector (banks, some telephone and trucking companies, for example) also be brought under the sway of the *Privacy Act*. Since this recommendation was one of the few made by the committee and not concurred with by the Privacy Commissioner, some explanation is in order, though the essential argument was made in an earlier report.

A broadening of the *Privacy Act's* universe beyond government would, of course, be justified by demonstrable and endemic abuses of privacy.

Indeed, there have been inquiries as to whether banks, telephone and cable television companies are covered by the *Privacy Act*. Sometimes anxious inquiries and public apprehension focus on the adequacy of privacy protection of credit card transactions.

The possibilities of violation are enormous and such nervousness is entirely prudent. Yet, while the dangers are real, the heavy hand of regulation should only be imposed if the private sector does not voluntarily take steps to address them.

Banks and their credit card associates, for example, have recognized that a high standard of privacy protection is simply basic good business. Thus, along with other businesses, they are developing, albeit slowly, their own codes of fair information practice. Privacy codes have also been adopted by the cable television, insurance, direct marketing and information processing industries.

In another business sector, at the initiative of the Canadian Radio-Television and Telecommunications Commission, privacy protection provisions have been written into new telephone company regulations. The CRTC's action provides a model for other regulators.

A sectoral approach is being increasingly advocated and practiced. It is becoming recognized as the model for the next generation of privacy laws. It is consistent with the fashion, perhaps the trend, towards decentralization and self-regulation.

One international indicator of the new trend is the Netherlands' new Data Protection Bill which allows organizations or business sectors to draw up privacy codes and submit them to the data protection authority for review. The authority can give the code a "declaration" —in effect, a seal of approval — if it finds the code conforms with the legislation. Needs and, as noted earlier, dangers differ.

Won't Suit All

The general principles enunciated in broadly-applied legislation may not well serve diverse groups. For example, it is highly doubtful that the *Privacy Act*, however ingeniously (or monstrously) elaborated, can be an effective code of fair information practice at the same time for, not only video stores, but the direct mail industry, credit bureaus and cable television.

Thus do arguments for extending the *Privacy Act's* domain to the private sector at this time go against the grain. They seem more doctrinaire than based upon hard evidence of abuses. To push privacy legislation where it is not necessary would cause it to be held cheap, to make it a burden rather than something valuable.

It would also require a greatly expanded Office of the Privacy Commissioner. Were the Act to cover all federally-regulated private sector firms, some 25,000 new institutions would be included. Even if the Act were to be applicable only to firms with 500 or more employees, 800 or 900 firms would be affected. Such an extension, by conservative estimate, would require a three to four-fold increase in human and financial resources in the Commissioner's office. Privacy protection would become big and expensive business. No one would gain from that.

Thus, there is no disappointment on the part of the Privacy Commissioner that the Crown corporations and no more have been brought under the *Privacy Act's* sway at this time. But the close call for the banks and the others in the federally-regulated category should be taken as notice. The handwriting in the parliamentary committee's report is a powerful incentive for the private sector to put its privacy house in order if it does not want legislation.

Assuming the private sector prefers a regime of voluntary to compulsory privacy regulation, scrupulous compliance with the data protection principles set forth in the guidelines of the Organization for Economic Co-operation and Development (OECD) would be a good place to start. Canada has endorsed the OECD's guidelines. The principles comprise essentially the same code of fair information practices as set forth in the *Privacy Act*. The minister of external affairs has called Canada's endorsement to the attention of major Canadian companies and urged that the OECD guidelines be put into practice. So far, the impact of this request is not discernible.

A few more steps

Though it risks turning too much of this report into a gloss of *The Steps Ahead*, a few more significant initiatives should be noted.

The government's statement, "Individuals cannot assert their rights under the *Privacy Act* unless they are aware of them", is a tautology which needs saying. The promised public awareness program will fill a long-felt need.

Almost five years after coming into effect, the *Privacy Act* probably still remains more unknown than known to Canadians. Yet, even with this general state of unknowing, some 170,000 individuals have applied formally under the Act to receive their personal information. These impressive figures immediately demonstrate the use-

fulness of the Act. What will the numbers be following a vigorous publicity campaign? (Will privacy be advertised as effectively as "Participaction"?)

A little background to another useful initiative announced in *The Steps Ahead*. Section 37(1) of the *Privacy Act* says that "the Privacy Commissioner may, from time to time" at his discretion, "carry out investigations ...to ensure compliance" with the Act's broad principles.

The Steps Ahead says "such audits are desirable" arguing that the *Privacy Act* does not "expressly authorize the Privacy Commissioner to conduct compliance audits on a regular and ongoing basis". The Act leaves compliance auditing to the Commissioner's discretion. The report announced that the Act will be amended to make the authorization explicit.

Such an amendment will be welcome, not because any institution has even slightly questioned the authority to carry out an audit. Nor has the Privacy Commissioner felt at all inhibited about initiating audits. (Why would the Act give the discretionary authority if it were not to be exercised?)

No, an explicit injunction to audit regularly sends the message that the Privacy Commissioner's compliance auditors will be coming. That message is important because regular, systematic auditing is the wave of the future for privacy protection. It offers the greatest source of privacy comfort —inside and outside of government.

However, privacy audits in federal institutions conducted by internal, departmental auditors have not developed as quickly as they should. Most departments have still to accept the argument that privacy audits should be as routine and necessary as financial or management audits. Yet without privacy audits it is difficult to understand how the heads of the institutions, who are responsible for implementing the *Privacy Act*, can be sure that their departments are complying.

Only a handful of departments are known to be conducting some internal privacy auditing: Environment Canada, the Bank of Canada and, in the last year, Employment and Immigration Canada (EIC). If an organization as large as EIC, and which handles as much personal information as EIC can take on the daunting task of critically examining its own privacy practices, what excuse can there be for others? Sadly, they appear content to await the coming (for some, it will be a long wait!) of auditors from the Privacy Commissioner's office for their privacy check-up. That may be flattering. But these specialist auditors should not be doing basic departmental tasks; they should be auditing the internal auditors.

The essential role of privacy coordinators to the effective functioning of the *Privacy Act* is clearly asserted in *The Steps Ahead*. That is welcome support for they are the privacy professionals, the privacy consciences of their institutions. They are sometimes pulled by a conflicting loyalty to their

colleagues and institutions on one side and to the abstraction called data protection on the other. That is why they should be persons of strength and status. They should have direct access to senior officials. Now the government too says that this should happen. Score at least two for the privacy coordinators!

These admirable fresh privacy initiatives set out in *The Steps Ahead* would be only posturing without the will and resources to carry them forward. It is too early to give out final grades, but the action plan for putting the new policies into effect has about it an encouraging look of rigor.

The tougher SIN and data-matching policies have been produced as promised. Others seem to be under way: for example, strengthening personal data protection provisions in the new security policy; a training regime so that federal public servants, notably privacy coordinators, may better discharge their responsibilities under the *Privacy Act;* putting in place by the Treasury Board of a new public awareness program. The Privacy Commissioner's staff is participating with Justice and Treasury Board officials in orientation sessions across the country at head offices of the Crown corporations coming under the mandate of the *Privacy Act.*

Other commitments will require more time. These include important *Privacy Act* amendments that will give unequivocal privacy protection to the personal information of public servants; provide a specific public education mandate for the Privacy Commissioner's office; facilitate the extension of the *Privacy Act* to some Crown corporations, such as Petro Canada.

When all these policies and amendments are finally in place, Canada's third-generation privacy legislation will continue to be as good as any in the world. No apologies needed.

What didn't happen

Yet a few more changes which the government's response did not address could make the good better. The greatest disappointment is that no commitment was made to provide a mechanism in the *Privacy Act* for an individual to prevent the release of personal information pending resolution of any dispute over the appropriateness of the release. The point is this, as made in last year's report:

> "It is an anomaly that individuals denied access to their personal information may go to court for review of the decision, but they cannot seek a review of a department's decision to disclose their personal information to third parties".

From anomaly to incongruity: the *Access to Information Act* provides a mechanism for notice to and comment by corporations whose sensitive commercial information may be released. Yet, the *Privacy Act* accords no similar rights to individuals whose sensitive personal information may be disclosed. Personal information deserves protection from abuse that at least equals that afforded corporate information. Amendments to the *Privacy Act* should end the incongruity.

Now back to the old vexation of section 19 of the *Privacy Act*, somewhat less vexatious than when first raised four years ago, but still an untidy, unsatisfactory business. Under section 19, federal government institutions *must* refuse release of any personal information received in confidence from a province. In 1983, most provinces, nervous and defensive, claimed confidentiality over all information already supplied to federal departments as well as information to be supplied in the future.

These blanket claims of confidentiality were a standing rebuke to the spirit of the *Privacy Act*. They have proved particularly troublesome in the parole and corrections field. Applicants are routinely refused information from their files at Correctional Services Canada (CSC) and the National Parole Board (NPB) only because it has been supplied by a provincial or municipal police force or a provincial parole or correctional service. CSC and NPB cannot release even the most innocuous information, which would be routinely released had it originated federally.

Rather than simply dismiss many complaints because federal departments have no choice but to withhold information, the Privacy Commissioner encouraged CSC and NPB to seek provincial agreements that would permit information to be processed under the *Privacy Act* as if it were federal information.

It Worked... sort of

The strategy produced some encouraging results: arrangements have now been made with Quebec, New Brunswick, Nova Scotia, Prince Edward Island and the Yukon. However, other provinces have not agreed. Ontario's case is particularly disappointing and curious because as of January 1, 1988, it proclaimed its own legislation to provide rights of access to personal information. The Ontario bill gives the province discretion to provide access to confidential federal information, as if it were its own — a curious double standard.

Unfortunately, no longer is there any reasonable expectation that the Commissioner can resolve complaints on information from Ontario, Manitoba, Saskatchewan, Alberta or British Columbia. Cases have too long been delayed already out of that hope. Now, there is no choice but to allow the use of section 19. It means geography will determine privacy rights. Some individuals will be granted access to personal information supplied by certain provinces; others will be denied access to similar information supplied by other provinces. That is essentially wrong.

There is a last hope — the political level. An agreement among the minister of justice, the solicitor general of Canada and all provinces could yet end this arbitrary discrimination. The cause is worth another effort.

As the finishing touches are applied to Canada's third generation of data protection rules, the focus shifts to new pressing privacy issues.

Towards an AIDS Policy

Perhaps the most sensitive and anguished privacy issue arises from our national response to acquired immune deficiency syndrome (AIDS). In what situations, if indeed any, is compulsory AIDS testing to be permitted? How should government use AIDS-related personal information which it holds? To whom and in what circumstances may AIDS-related personal information be disclosed? Does the stigma of AIDS require that it be treated differently than other communicable diseases? What level of physical security should AIDS-related information receive? These are fundamental questions to the development of a federal privacy policy on AIDS information.

Such policy should be developed by government, by legislators, not by the Privacy Commissioner. He will press the privacy interest — vigorously. But many competing concerns must be considered by those with overreaching responsibilities.

Based on the assumption that a lack of information should not prevent development of a coherent, sensitive privacy policy on AIDS, the Privacy Commission has initiated a study of AIDS from the privacy perspective so as to provide the best and latest advice. Key government departments gave full cooperation to this study.

The federal umbrella confronts the issue of AIDS on many fronts — in its dealings with prisoners, immigrants, its own employees (be they foreign service officers, members of the armed forces, prison guards or nurses). While Health and Welfare Canada encourages employers to establish AIDS policies, the country's largest employer — the federal government — has as yet no such policy of its own.

Absence of a general policy does not mean that AIDS testing programs have not been implemented. For example, National Defence has begun an AIDS-testing program to meet a requirement established by the U.S. Defence Department. This American policy requires all foreigners attending U.S. defence training courses to certify that they do not carry the AIDS antibody. More than 1,000 military and civilian employees of Canada's National Defence department attend these courses annually.

It is open to serious question whether U.S. policy on AIDS testing should drive Canadian policy. But the fall-out cannot be avoided. For example, should Canada reject mandatory AIDS testing, what would be the impact on the careers of employees denied access to U.S. defence training courses because either they refused to be tested or they tested positive?

If Canadian policy encourages only voluntary AIDS testing, then a clearly defined policy should be issued indicating how such information will be used and the circumstances under which it may be disclosed to third parties.

CSIS Files

Another unresolved issue of much discussion this past year is the balance to be struck between accessibility and secrecy in security and intelligence. The Canadian Security Intelligence Service (CSIS) is subject to the *Privacy Act*. However, few applicants have been given access to their files or have ever received confirmation whether a file on them exists. This should come as no real surprise to anyone; silence is in the nature of CSIS's business. There has been no pattern of non-compliance by CSIS with the *Privacy Act* and Parliament specifically provided exemptions for disclosure requirements, recognizing the special circumstances of security and intelligence work.

But there comes a point, either as time diminishes the sensitivity of information or because of its seemingly innocuous nature, where it becomes difficult to explain how the release injures CSIS.

This issue is being explored, with the co-operation of CSIS, with the aim of achieving a clearly defined and acceptable policy.

Welcome to the Club

Important Canadian privacy news of the year was not confined to the federal domain.

The coming into force of Ontario's *Freedom of Information and Protection of Privacy Act* advances significantly the quality of data protection in Canada. Covering provincial institutions as it does, Ontario's new law confers important privacy rights upon millions of individuals.

Cordial, close working cooperation has already been established between the office of the Ontario Commissioner, Sidney Linden, and that of the federal commissioner. Visits have been exchanged and useful consultations have taken place.

Strong provincial data protection statutes (Quebec's comprehensive law came into force in 1984) will be mutually re-inforcing both for the provincial and federal laws. Privacy, like freedom, should not be divisible.

ISSUES — Old and New

DATA MATCHING AND SIN

At the beginning of this report, the government's important commitment to establish controls on data matching and on the use of the SIN was included among the good privacy news of the past year.

The power, versatility and omnipresence of information processing technology are perhaps the greatest challenge to the effectiveness of the *Privacy Act* in the decade ahead.

A prime goal of the *Privacy Act* was to erase the possibility of the government establishing one central, comprehensive information file on any single individual. The central file possibility has reached technical feasibility as government holds more information in machine readable form. By using the Social Insurance Number (SIN), the government's personal identifier, computer matching techniques would accomplish what previously was felt — perhaps too smugly — to be most unlikely.

The government's commitment is therefore timely. The Privacy Commissioner's office has worked closely with Treasury Board officials responsible for drafting a detailed control policy. Canada could very well have the world's most rigorous controls on the use of computer technology to compare and compile information extracted from records contained in unrelated data bases.

Data Matching Policy

The major features of the new data matching policy are:

* no data matching shall be undertaken except with the written approval of the head of the government institution involved, which, ordinarily, is the minister;

* all proposed data matches will be appropriately documented including:

  — a preliminary assessment of a match's compliance with the *Privacy Act*, and

  — a further assessment of the costs and benefits of the proposed match against an analysis of the potential threat to the privacy of individuals;

* all data matching will be described in the Index of Personal Information;

* proposed data matches must be submitted to the Privacy Commissioner 60 days before the match is to begin;

* any information generated from data matching must be subjected to independent verification before being used in a decision-making process that directly affects an individual; and

* an individual must be given the opportunity to refute the information resulting from data matching before any action concerning the individual is initiated.

SIN policy

The government's commitment to return the SIN to its intended role as a specialized identifier for selected social programs is critical to data matching control. Only those programs authorized by Parliament to do so will use SIN. Gradually, other programs will replace SIN with unique identifiers, reducing the possibility of matching information from unrelated data bases by making it far less cost effective.

The new SIN policy will:

* freeze further collections and uses of the SIN by government, unless authorized by Parliament;
* review all existing collection and uses of SIN to ensure compliance with the *Privacy Act*;
* require that all not statutorily mandated existing collections and uses of SIN be discontinued unless the Treasury Board believes that the benefits of continued collection and use of SIN would outweigh privacy concerns;
* permit no right, benefit or privilege to be withheld, nor any penalty imposed on an individual for refusing to provide a SIN, except where collection is required by statute;
* inform individuals of the purposes for which a SIN is requested, whether disclosure is mandatory or voluntary, and whether there are any consequences resulting from failure to provide.

While these initiatives are welcome, Parliament could yet override the policies and the *Privacy Act* by authorizing new computer matching programs and new uses of the SIN. The U.S. Congress, for example, has authorized widespread computer matching, particularly to detect and prevent defrauding government programs.

It is difficult to argue persuasively against this purpose and in Canada, too, it may be an important force for the proliferation of data matching. However, there is growing U.S. evidence that computer matching produces less significant savings than previously claimed. Proper program design and alternative enforcement techniques are as cost effective as data matching, and eliminate the consequent invasion of the privacy of innocent individuals.

As has been stated, other social "goods" may outweigh privacy. But it is for Pariament to make these judgments on the most informed basis possible. One critical piece of information is a rigorous cost/benefit assessment of any proposed new data matching activity. However laudable the social purpose Parliament should not authorize matching activity without weighing the costs and benefits against the potential invasion of privacy.

"CONSISTENT USE"

Now that both the *Privacy Act* and the new policy restrict data matching, government departments may be tempted to interpret "consistent use" broadly enough to match unrelated files.

The *Privacy Act* has no mechanism for the Privacy Commissioner (or anyone else) to challenge misuse of information in the courts. Departments could use the "consistent use" provision to undermine effective control over data matching.

The Ontario *Freedom of Information and Protection of Individual Privacy Act* attempts to prevent too broad an interpretation by including a definition of "consistent purpose". Section 43 of that act provides:

> "Where personal information has been collected directly from the individual to whom the information relates, the purpose of a use or disclosure of that information is a consistent purpose ... only if the individual might reasonably have expected such a use or disclosure."

Thus, the Privacy Commissioner recommends two amendments to the *Privacy Act:* a definition to clarify interpretation of "consistent use"; and authorization for the Privacy Commissioner or any aggrieved individual to seek judicial review of a government institution's decision to use or disclose personal information.

The difficulties which lie ahead in taming technology to the principles of privacy should not overshadow the importance of the controls which were referred to earlier.

PAROLEES, INMATES AND PRIVACY

As promised in last year's annual report, the Privacy Commissioner reviewed the use and disclosure policies of the National Parole Board (NPB) and Correctional Service Canada (CSC). NPB gave the Commissioner a revised draft use and disclosure code for review. CSC policies were examined during the privacy audit described elsewhere in this report.

From the review the Commissioner identified three matters which he considered infrigements of the *Privacy Act.* They governed disclosures to the RCMP, to victims and to the media and public.

Disclosures to the RCMP

The NPB and CSC disclosure policies authorize the release of parolees' and inmates' personal information to the RCMP, considering all such disclosures a "consistent use" of the information (paragraph 8(2)(a) of the *Privacy Act*). This does not recognize that the RCMP may be seeking information concerning a crime unrelated to the one for which the individual was sentenced.

CSC and NPB do not follow the *Privacy Act's* direction that disclosures to the RCMP be made only on written request, specifying the purpose and describing the information sought. Copies of these requests and a record of the information disclosed must be given to the Privacy Commissioner at his request.

As the two agencies consider all disclosures to the RCMP "consistent use", neither requires written requests nor does it keep records of disclosures for the Privacy Commissioner's review.

Even if RCMP requests are "consistent", the *Privacy Act* requires them to describe the uses in the Personal Information Index and, in the absence of a listing, to notify the Privacy Commissioner of the disclosure and its purpose.

Never has the Privacy Commissioner been notified of disclosures to the RCMP even though they occur routinely. Moreover, many of the relevant CSC and NPB Index descriptions do not advise that disclosures may be made to the RCMP.

This behavior clearly inhibits the Commissioner's independent scrutiny of disclosures specifically required by the *Privacy Act*.

Disclosure to Victims

NPB and CSC have a policy of telling the crime victim the date of an inmate's release, conditions of the release, and his or her destination, considering such disclosures as consistent uses by paragraph 8(2)(a).

The Privacy Commissioner disagreed. Only when there is reason to believe that the person would harass, harm or otherwise put the victim at risk would the release be a consistent use, or clearly in the public interest (subparagraph 8(2)(m)(i) of the *Privacy Act*). Both the NPB and the CSC were encouraged to assess each case individually rather than give blanket approval for such releases.

The release of personal information to third-parties violate inmates' privacy rights and could jeopardize their reintegration into the community and, even, put them at risk.

CSC and NPB have agreed to develop a new policy on disclosures to victims which provides a much greater degree of control over such releases.

Disclosures to the Media and Public

The NPB and CSC policies previously authorized the release of an offender's criminal record to the media and the public. Both agencies considered an individual's criminal record to be unprotected by the *Privacy Act* because the information is publicly available in court records.

The Privacy Commissioner disagreed with this interpretation since it would mean that the criminal records of anyone could be assembled and disclosed to the general public — an unacceptably broad interpretation of what is meant by "publicly available".

An individual's conviction may indeed be recorded in publicly available court records, scattered perhaps across the country (and out of the country). However, this should not mean that a cumulative listing of convictions, prepared by a law enforcement or correctional institution, is also public. The

impact of cumulative records is quite different and distinct from a record of an individual conviction, particularly because they differ both quantitatively and in the consequences of their release. This is all the more so since cumulative records are more susceptible to inaccuracy and incompleteness.

It should also be noted that the Solicitor General has a strict policy of confidentiality for the RCMP as the national custodian of criminal record information. That policy authorizes no disclosures to the public or media.

Subsequent revisions by CSC and NPB to the policy have removed the authorization for the public release of an offender's criminal record.

PRIVACY IN THE WORKPLACE

Workplace issues will increasingly consume the Privacy Commissioner's time and attention as Crown corporations and their subsidiaries come under the jurisdiction of the *Privacy Act*. The combined workforce of the 130 additional institutions is greater than the 147 institutions already covered by the Act. An added complication is that some of the major Crown corporations (such as Air Canada and Petro Canada) compete in the private sector where few privacy rules apply and employee screening and monitoring are more widespread.

During the year public servants became worried that too much information about them was accessible under the *Access to Information Act*. They were concerned, for example, that management was seeking too many details about their medical conditions; that long-time public servants were having to undergo new, rigorous reliability and security clearance checks; and that drug testing, AIDS testing and electronic surveillance could strip them of personal privacy and dignity in the workplace.

Accessibility to Employee Data

The Commissioner's 1986-87 annual report summarized an investigation into the compliance of the government's *Conflict-of-Interest Code* with the *Privacy Act*. The Commissioner found that the *Privacy Act* may not protect personal information about public servants from disclosure to third parties under the *Access to Information Act*.

There were several complaints launched this past year about disclosures of public servants' information under the *Access to Information Act*.

For example, both the Department of National Defence (DND) and the RCMP released lists of all members and civilian employees in the National Capital Region who were earning $42,000 a year and above, their rank, classification and their area of service within the department. In these instances, described in detail in the report's complaint section, the Privacy Commissioner concluded that such

information is not "personal" according to section 3(j) of the *Privacy Act* and cannot be protected. In fact, the departments are required to disclose the information. However, individuals should not be sitting ducks for commercial solicitation because they happen to be public servants. As in the conflict-of-interest investigation, these disclosures simply emphasized the need for a greater protection of information that the government holds about its employees. This is particularly critical for public servants working in sensitive, high security jobs whose safety could be threatened by the mere fact of their public identification.

The government discussed these concerns in *The Steps Ahead*, promising amendments to the personal information definition ..."to ensure that sensitive employee information, such as employment equity or conflict-of-interest declarations and employment appraisals, is treated as personal information and subject to the protection of the *Privacy Act.*"

This amendment will not, however, resolve departments' dilemma when faced with request for lists of employees for commercial or soliciting purposes.

Disclosure of Medical Data

One public servant complained when he was denied sick leave benefits for refusing to give his superior the details of his illness or disability. The department argued that it needed the information because of the amount of sick leave already taken, concern over the employee's physical well-being and its affect on the safety of the employee and others in the workplace, and the possible implications for long-term disability.

The Privacy Commissioner did not question the employer's need for evidence that the employee was unable to perform his duties due to illness or injury. However, collecting precise details of an illness, injury or other medical conditions is prohibited by section 4 of the *Privacy Act.* Employers questioning employees' sick leave claims can verify the medical status and fitness for work through a Department of Health and Welfare doctor.

The department agreed to this policy and the Privacy Commissioner recommended that all government institutions implement a similar approach.

Reliability and Security Screening

The Privacy Commissioner reported last year that while the government's new security policy did not contravene the *Privacy Act,* it left little to individual departments' discretion. This lead to the spectacle of fingerprinting the staff shovelling snow from the skating rinks on Ottawa's Rideau Canal. After discussions with Treasury Board, the policy was amended to give departments the discretion to determine when credit and fingerprint checks would be a necessary part of an enhanced reliability check.

However, protection of the public servant's information collected under the policy should be addressed as part of the statutory amendment to the definition of personal information (see sample complaint on page 29). The Privacy Commissioner is also concerned that there may be too many public service positions requiring their incumbents to be security-cleared. Since security clearances to confidential, secret or top secret levels involve detailed background investigations, only those individuals whose duties truly require such clearance should be subjected to them. The Privacy Commissioner will be examining this matter to ensure that security clearances are not an arbitrary requirement.

AIDS testing

No one can ignore this as yet incurable and fatal disease, the acquired immune deficiency syndrome (AIDS). It is having an effect on all levels of our society and raises troubling, complex issues.

In responding to the AIDS epidemic, government policies and initiatives should balance two important and at times competing objectives: the protection of individual rights and the protection of the public health.

The government's collection, use and disclosure of AIDS-related information should, of course, comply with the *Privacy Act*. But should this category of medical information be treated differently than personal information about other communicable diseases? *Does the Privacy Act* prohibit or restrict mandatory AIDS testing? To what uses may AIDS-related information be put, to whom may it be disclosed and for what purposes.?

Since the legal requirements are not clearly defined and a number of difficult questions need to be explored, the Privacy Commissioner has undertaken a study in close consultation with key government departments. A discussion paper is being prepared which should help the development of a policy on AIDS-related information which is both sensitive to privacy rights and the protection of public health.

Employee screening

The *Privacy Act* does not deal specifically with such screening and monitoring techniques as drug and polygraph testing and electronic surveillance. The Parliamentary Committee recommended that the Act be broadened from simply data protection, to include physical privacy and to give the Privacy Commissioner the authority to monitor developments in surveillance techniques. The government rejected this recommendation, believing that the *Privacy Act* should remain as a data protection statute and regulate only the collection, use and disclosure of the personal information produced by surveillance and tests.

The Act does deal adequately with the use and disclosure of results. However, compliance with the provision that government not collect personal

information unless it "relates directly to an operating program or activity" (section 4), continues to pose questions. Perhaps the most important one concerns the reliability of screening methods because the use of unreliable screening tests could itself contravene section 4. Similarly, intrusive screening, testing and monitoring techniques may represent prohibited forms of data collection if other, less intrusive, methods are available options.

The Privacy Commissioner will continue to watch closely the government's monitoring and testing of applicants and employees and will encourage the development of guidelines to protect individuals' privacy interests.

Exempt banks

Compliance audits on five remaining exempt banks found only one, National Defence bank DND/P-PU-040 (Security and Intelligence Information Files), properly constituted. (To be properly constituted, each file in the bank must be reviewed to ensure it consists "predominantly" of personal information whose release could injure Canada's international affairs, defence or law enforcement, or was obtained by an investigative body.)

The other banks listed as exempt in last year's report with the exception of RCMP bank CMP/P-PU-015 (Criminal Operational Intelligence Records), are now treated as open and their exempt status will be rescinded.

The Privacy Commissioner found the RCMP's remaining exempt bank too had not been properly constituted. He recommended the Solicitor General rescind the existing exempt bank order and seek a new, valid order if the Minister considers it necessary to maintain the bank's exempt status. The Solicitor General has disagreed, believing that all of the files which the Privacy Commissioner found not reviewed originally were not, in fact, part of the exempt bank.

Discussions toward resolving this factual dispute are in progress. In the meantime, the Solicitor General will maintain the exempt status of RCMP bank CMP/P-PU-015.

Complaints Branch

The office received 696 complaints during the year; 661 investigations were completed of which the Commissioner concluded that 155 (23 per cent) were well-founded and 492 (74 per cent) were not well-founded. The remaining 14 (3 per cent) were abandoned or withdrawn.

Compared with 1986-87 statistics, two changes are worthy of note. First, there has been a marked drop in delay complaints. Delay complaints account for 22 per cent of the caseload; the previous year they accounted for 56 per cent. This somewhat surprising change is responsible, in large measure, for this year's smaller proportion of well-founded decisions; delay complaints have usually been justified.

The second change is that 66 (8.6 per cent) fewer complaints were lodged than in the preceeding year. For the first time in five years complaints have not risen by at least 10 per cent. While any reduction in complaints should be viewed positively — the ultimate goal, after all, is to have departments satisfy all users of the Act — the statistics do not necessarily reveal an entirely comforting story.

True, applications are now being handled by departments in a more timely fashion. There has been, however, a significant shift to more substantive complaints.

Almost 64 per cent of the year's completed complaints concerned denial of access to personal information. Compare this with only 36 per cent last year. The somewhat disturbing development is the sharp increase in situations where departments have refused to provide requested information, not simply been tardy in processing a request. One year's figures do not make a trend but the rise in access denials will be carefully watched.

While the caseload for each of the seven investigators averaged a seemingly more manageable 99 for the year, down from 109 the previous year, the investigative effort required to complete the more complex caseload has in fact increased. In addition to the investigation of complaints, investigators also handled 1,248 inquiries, an increase of almost 10 per cent from the previous year (see page 46).

In total this represents an unsustainable work burden on investigators which would lead to an unacceptable backlog of cases. For this reason, as well as the anticipated new business from the Crown corporations being brought under the Act, it is encouraging to report that approval has been given for nine additional staff, including investigators.

The following cases illustrate the types of complaints the office dealt with during the year. Identifying details are removed because the Act requires that investigations be conducted in private.

COMPLAINTS

Commercial Use of Data

The vexed issue of releasing lists of departmental employees' names for commercial purposes commanded attention during the past year.

The concern can probably be best illustrated by the military officers who complained that releasing a list of National Defence personnel to an Ottawa man contravened the *Privacy Act*. The complainants concluded that the lists had been sold when they began receiving solicitations from a local real estate developer.

The man applied under the *Access to Information Act* for a list containing the "name, rank, job classification and level, office address and branch or unit" of all civilian employees and Armed Forces personnel in the National Capital Region "whose salary range equals or exceeds $42,000 per annum."

Personal information may not normally be released under the *Access to Information Act*. The company's agent himself questioned whether obtaining this type of information violated the *Privacy Act*. However, the Act is clear; information about public servants' positions, functions and salary ranges, and their titles, business addresses and phone numbers is not "personal". This exception set forth in the *Privacy Act* establishes in law the public's right to know who is paid from the public purse, and for what. The investigation, therefore, hinged on the interpretation of the definition of personal information about federal government employees.

The Commissioner concluded that DND was compelled to release the personal information and that he had little choice but to dismiss the complaints because the wording of the Act is clear. But the issue is troubling. Federal employees should not become targets for repeated canvassing for various goods and services. That possibility could not have been contemplated by those who drafted the *Privacy Act*.

There is even a potential security problem in releasing the names of staff and Armed Forces members. Many work in sensitive positions and they are not even listed in DND's own directories.

Following his investigation, the Commissioner wrote to the deputy minister of national defence to share his concern that "personnel working in particularly sensitive high security areas could be identified by hostile interests." It was pointed out that computer manipulation of particular lists could determine how DND "allocates its personnel by rank and location, thus inferring what military or intelligence priority it is giving to various activities and projects." The Commissioner asked DND to support an amendment to the *Privacy Act* closing this loophole. (See also next case).

Ditto RCMP

The security issue arose again in similar complaints from members of the RCMP. The police force had complied with an application almost identical to the request handled by DND. However, an RCMP staff relations representative expressed to the Commissioner "grave concerns" about the information "falling into the wrong hands".

The letter went on:

> "The very nature of police work exposes members to possible reprisals by...terrorists, drug dealers and cop haters whose exploits fill our newspapers daily. Any member who is now working or has previously worked in the areas of drug enforcement or anti-terrorism will confirm that information such as work locations and business telephone numbers could, in criminal hands, jeopardize police operations and place both individual members and their families at risk."

The Commissioner reiterated his conviction that "a greater measure of protection should be given to information held by government about public servants." He recommended that Parliament amend the language of the section to make it clear which information about public servants should be considered public — and which should not. Until the definition has been tightened up, as promised in forthcoming amendments to the Act, departments should have a discretion to withhold certain job-related information about public servants when security is at issue.

Officer Gets Merit List Ranking

An Armed Forces officer complained to the Commissioner when DND would not tell him exactly where he stood on a promotion list. Such lists are prepared annually by merit boards which review all eligible members within each rank and occupational group.

National Defence did provide the officer with a computer-listing page containing column headings and his one-line entry. There was nothing to indicate his position on the otherwise blank page. He was told that DND had discontinued numbering positions in 1978 and, without numerical rankings beside each name, the department maintained it could not provide the information since it did "not exist on the record".

As a former career manager, the complainant said he knew managers often assigned numbers to promotion lists and, in fact, had been told his position every year from 1980 to 1985. As well, he believed the page number on the copy was wrong.

DND acknowledged that some members had been given their rankings in the past, but maintained that as word of the practice spread it became too time-consuming to respond to all the requests and the practice was stopped. The privacy investigator was told that although the department could determine an officer's position simply by counting down the list, it was not required to do so because the information "is not recorded or compiled in any form" and, therefore, does not qualify as personal information under the *Privacy Act*. (The staff also reiterated that the page number was correct.)

The investigator confirmed that the list was assembled "in order of merit" and that it was used to make administrative decisions about the individuals on such matters as promotion, attendance on courses and suitability for employment.

The investigator suggested that an officer's position on the list would come under the definition of personal information in the *Privacy Act* which covers "any identifying number, symbol or other particular assigned to the individual".

The discussion see-sawed back and forth over several months. The investigator examined the promotion list to confirm that there was no numerical ranking, and determined that the page number — as the complainant maintained — was wrong. The error was corrected.

The Commissioner alerted the deputy minister to a preliminary finding that the complaint was justified because the list contained two items of information about the individual: that he is on the list, and his standing relative to others on the list. The Commissioner wrote: "...to refuse to disclose X's exact position on the list, merely because no number corresponding to that position appears on the list, effectively deprives X of one piece of his personal information contained on the list."

In September 1987 the Chief of the Defence Staff advised the Commissioner that, upon review, DND changed its policy on releasing a merit list position.

"Commencing with the 1987 merit boards, a position number will be added to the merit lists..." the Chief wrote. Beginning January 1, 1988, applicants will be given both their merit list standing and the total number of members considered by the board.

The letter included where the complainant stood on the 1987 promotion list.

UI to Limit Pension Queries

An Ontario man complained about the pension coverage questions he was asked to answer when he applied for unemployment insurance.

The document, called a "fact-finding questionnaire", asked the unemployment insurance applicant to describe his pension coverage, including the source, the type of payments and the payment schedule, whether pension payments had been converted to RRSPs, annuities "or any other type of savings or investment plan, account or program".

During the investigation, Employment and Immigration Canada's (EIC) staff said that a 1986 amendment to the *Unemployment Insurance Act* provided that claimants receiving pension benefits could have their UI benefits reduced. The questionnaire, they said, was to determine whether applicants were receiving pension funds. Thus, the information related to administering the unemployment insurance plan and, as such, was permitted under the *Privacy Act.*

The Commissioner agreed that this rationale would be true if the questions concerned the period when the applicant was unemployed. However, the questions were completely open-ended, leaving applicants feeling obliged to reveal details about pension coverage that may be years away from producing benefits. He told EIC the collection of this information seemed premature.

EIC agreed to add a footnote to the questionnaire, limiting the pension queries to the period of unemployment and said that a new national questionnaire, without footnote, was to be introduced.

After three months of discussions, EIC agreed to add the limiting statement to the new form. Unfortunately, the man whose complaint changed the policy moved, left no forwarding address and never heard the good news.

Medical Information — Canada Post

A postal employee complained that Canada Post had improperly disclosed information to his physician, had obtained personal information from his physician without his permission, and had used a medical report filed during a compensation hearing to prevent his return to work.

Origin of Completed Complaints by Province and Territory

Newfoundland	3
Prince Edward Island	2
Nova Scotia	13
New Brunswick	8
Quebec	219
National Capital Region Quebec	4
National Capital Region Ontario	107
Ontario	131
Manitoba	30
Saskatchewan	25
Alberta	57
British Columbia	53
Northwest Territories	4
Yukon	1
Outside Canada	4
TOTAL	**661**

Investigation confirmed that Canada Post had referred to the medical report they had received at the hearing when they refused his attempt to return to work. The information bank containing the report ("Occupational Health and Safety"), is described as containing information used "to establish conditions under which employees...with identified illnesses or disabilities are able to continue to work...". The Commissioner concluded that Canada Post had not misused this information.

During the investigation, it was learned that Canada Post had obtained information from the employee's physician without his consent, but the request was made prior to the implementation of the *Privacy Act*, and therefore did not contravene the Act. It was also determined that a copy of correspondence containing personal information from Canada Post to the complainant had been sent improperly to the complainant's physician. Canada Post will ensure that this does not recur.

Leave and Medical Diagnosis

Two complaints were received about departments requiring detailed medical information from employees absent on sick leave.

In one case, cited earlier to illustrate the need for privacy in the workplace, a Department of Communications (DOC) supervisor had rejected both the standard sick leave declaration and a medical certificate, insisting on knowing the medical details which kept an employee away from work. The employee had a history of lengthy absences for health reasons.

While refusing to supply the information, the employee agreed to be examined by a Department of Health and Welfare doctor. The government doctor found the employee in good health, but was unable to determine what condition had prevented the man working because he was refused permission to speak to the man's personal doctor.

When DOC refused to pay for sick leave, the individual complained that requiring him to provide the diagnosis violated the *Privacy Act*.

DOC argued that it had the right to the information because of the number of health-related absences, the concern for both the employee's own and other employees' health and safety, and the implications for long-term disability cases. DOC also cited the employee's collective agreement and a grievance adjucation decision to support this argument.

The Commissioner agreed that the employer legitimately required evidence that an employee was medically unable to work before being granted paid sick leave. He also agreed that employers could refer an employee to a doctor of their choice to confirm fitness for work but, he said, "in my view it is not necessary for the employer to know the nature of the illness".

As a result, the department changed its policy, saying that in future it would not request details of employees' medical conditions. Fitness for work would be verified, if necessary, through a Health and Welfare doctor. No details on an employee's condition would be passed back to the department. DOC subsequently paid the complainant's sick leave.

Diagnosis removed from file

A Quebec City woman complained that, without permission, her employer (Employment and Immigration Canada) asked her family doctor for medical details after she submitted a certificate of disability. The details then became part of her personnel file.

EIC explained that managers often reach employees' doctors in order to determine what work can be performed by an employee with health problems, but not to get details of their condition. This practice was said to be faster than waiting for employees to obtain the information themselves and, EIC said, the complainant knew they would call her doctor whether or not she agreed.

The Commissioner concluded that the onus is on the department to collect information directly from an employee or to get the employee's permission before reaching the personal physician. Even then, the only information an employer needs is the expected duration of the condition and any restrictions it could place on the employee when returning to work.

After months of negotiations, EIC agreed to remove the medical diagnosis from the file.

The Commissioner believes that the problem exists in other departments and urged Treasury Board to issue government-wide instructions consistent with the *Privacy Act*.

No Information to Police

An inmate complained that Correctional Service Canada had misused his personal information by giving his "penitentiary file" to a city police force. He alleged that the police then passed it to a Crown Attorney and a Crown psychiatrist before giving it to his lawyer.

The Privacy Commissioner's investigator could find no evidence that personal files had been passed around. The complainant produced a page copied from a court transcript in which the Crown psychiatrist cited tests and files on which he based his assessment of the inmate. One of the items was described as "police reports and penitentiary service files".

While the Crown psychiatrist had seen files, this appeared to be a consistent use of the information since the hearing was to determine whether the inmate was a dangerous offender. There was nothing to prove that the information had been passed to the police.

The Commissioner found no evidence that personal information had been misused or improperly disclosed and dismissed the complaint.

Union and Security Checks

Three public service unions complained about Revenue Canada's implementation of the government's security and reliability checks. The unions said their memberships considered the collection of criminal records, financial transactions and fingerprints "illegal". They asked the Commissioner to investigate, in particular, Revenue Canada, Taxation's personnel screening policy.

Following the theft of tax microfiche (see page 10 — 1986-87 Annual Report), the minister of national revenue ordered immediate implementation in the tax department of the new government-wide security policy. The policy's basic reliability checks include verifying education and professional qualifications, employment data, performance and character assessments and a name check of the criminal records bank. The more rigorous "enhanced" security check also requires fingerprinting and a credit check.

The Commissioner found that Treasury Board had the right (indeed, the duty) to assess its employees' trustworthiness and loyalty to prevent the abuse or disclosure of taxpayers' personal information.

However, he continues to be concerned that third parties may apply to see individual security files under the *Access to Information Act*, given the limited protection for public servants' personal information. Following discussions, prompted by a similar complaint about the government's conflict-of-interest code, Treasury Board promised to ask Parliament to amend the *Privacy Act* to limit availability of public servants' personal information to name, salary-range, title, position duties and business address.

Treasury Board accepted the Commissioner's recommendation that deputy ministers be given discretion to decide whether fingerprinting and credit checks are reasonable and for which employees. The policy has been changed.

Tax Auditor Obtains Meeting Notes

A Revenue Canada tax auditor complained to the Commissioner when the department withheld material from a letter which accused him of a conflict-of-interest. He considered the edited pages to be "meaningless".

In a letter to the revenue minister, a man alleged that the tax auditor (his wife's first husband) was using his position to advantage in a legal dispute with the wife. The letter also mentioned that the auditor had recently caught one of the writer's fellow employees for unreported earnings, implying that the incidents were connected. The department's internal inquiries revealed no wrongdoing on the auditor's part.

An investigator persuaded the department to release more of the original letter. However, much of the exempted material was personal information about someone else. The exemptions were valid.

In the meantime, the complainant again wrote to the minister concerned that an internal inquiry would produce more documents than he had received. In a meeting with the departmental privacy coordinator, the complainant asked for any personal notes taken by managers during interviews for the internal conflict investigation as well as the investigation file. He also asked to review the tax file of the employee caught not reporting earnings.

The investigator negotiated the release of some meeting notes and a record of a phone conversation with the person who alleged the conflict-of-interest. However, the investigator confirmed that there were no other personal notes, no investigation file, and no references to the complainant in either the minister's letter reponding to the original complaint, or in the fellow employee's tax file.

The Commissioner upheld the complaint because the department had not provided all the material in response to the first request. The applicant now has the material to which he was entitled

Accepts Correction, Refuses Another

A Manitoba man complained that the RCMP had denied his request to correct factual information in a file obtained as a result of a *Privacy Act* request.

The investigator found that the RCMP had accepted one correction but denied the second because an RCMP officer had reported a different version of the incident. The complainant's comments were noted on the file.

In his letter to the complainant, the Commissioner explained that there is no clear method of resolving disputes in which there are different perceptions of an incident. Since the complainant's version is now on the file, the Commissioner considered the RCMP's response was reasonable.

Permission Prompts File Release

An Employment and Immigration Canada (EIC) employee, accused of conflict-of-interest in hiring, alleged that EIC had not provided all the material he had requested, had improperly collected information during the inquiry, and had delayed responding to his request.

EIC had not responded to the complainant's memo asking for copies of documents from the inquiry. However, he had not used the proper form, had not cited the *Privacy Act* and had not sent the request to the privacy office. Thus, it was not technically a formal privacy request and the department was not obliged to respond.

Once EIC received a formal request, it extended the deadline to the full 60 days so as not to "unreasonably interfere with the operations of the government institution". Since staff had to process a large volume of material, the extension was reasonable.

When he received the material, the applicant found information had been withheld because it concerned another individual (much of it about the person hired). He had also expected to receive his supervisor's notes from their meeting, material from the labour relations unit, interviews with staff members about hiring and relevant correspondence with the minister. When he found none of this material he complained to the Commissioner.

The investigator found the supervisor's handwritten notes were destroyed once his report was written. There was no material in the labour relations unit and notes from interviews with others had been properly exempted. The minister's correspondence, originally overlooked, was released. After the complainant obtained the third party's permission, EIC also released that information.

The Commissioner dismissed the complaint that EIC had collected the information improperly. Although EIC had made inquiries outside the department, including interviews with neighbours, existing case law gives employers considerable scope in ensuring employees are not involved in misconduct.

Completed Complaints by Department, Type, and Result

Department	Complaint Type	Number (Total)	Justified (Total)	Dismissed (Total)	Abandoned (Total)
Agriculture Canada	**Access**	**6**	**—**	**6**	**—**
Bank of Canada	Access	1	—	1	—
Canadian Commercial Corp.	**Access**	**1**	**1**	**—**	**—**
Canadian Human Rights Com.	Access	4	1	3	—
	Misuse	1 (5)	— (1)	1 (4)	—
Canadian Labour Rel. Board	**Access**	**6**	**—**	**6**	**—**
Canada Post	Access	23	4	19	—
	Misuse	2	1	1	—
	Correction	1	—	1	—
	Delay	1	—	1	—
	Col/Ret/Di	3 (30)	— (5)	3 (25)	—
Canada Ports Corporation	**Delay**	**4**	**4**	**—**	**—**
Correctional Service Cda	Access	104	12	88	4
	Misuse	7	—	7	—
	Correction	6	1	5	—
	Delay	39	33	5	1
	Language	9	1	8	—
	Col/Ret/Di	5 (170)	— (47)	5 (118)	— (5)

Completed Complaints by Department, Type, and Result

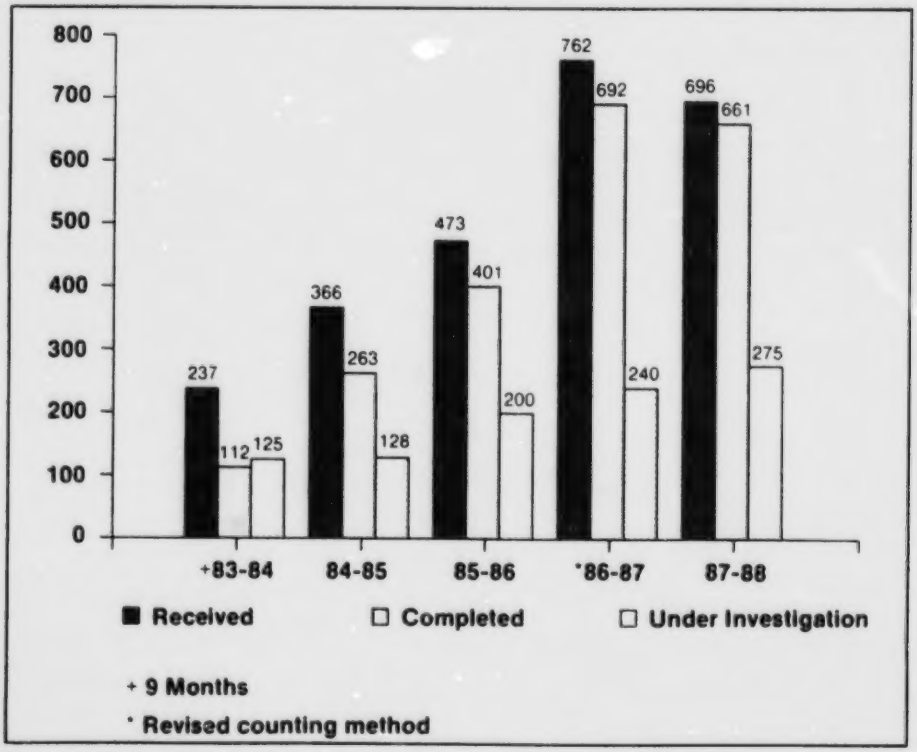
Department	Complaint Type	Number (Total)	Justified (Total)	Dismissed (Total)	Abandoned (Total)
Canadian Security Intelligence Service	**Access**	**20**	**1**	**19**	**—**
	Delay	**3 (23)**	**— (1)**	**3 (22)**	**—**
Canadian Transport Com	Access	3		3	
Communications	**Access**	**1**	**1**	**—**	**—**
External Affairs	Access	4		3	1
	Misuse	1 (5)	1		
Environment Canada	**Access**	**2**	**—**	**2**	**—**
Export Development Corp	Access	1		1	
Employment and Immigration Canada	**Access**	**62**	**11**	**49**	**2**
	Misuse	**4**	**—**	**4**	**—**
	Delay	**25**	**20**	**5**	**—**
	Col/Ret/Di	**5 (96)**	**1 (32)**	**3 (61)**	**1 (3)**
Health & Welfare Canada	Access	9	3	6	
	Misuse	3	1	1	1
	Delay	9 (21)	4 (8)	5 (12)	(1)
Immigration Appeal Board	**Access**	**1**	**1**	**—**	**—**
	Misuse	**1 (2)**	**—**	**1**	**—**
Indian & Northern Affairs	Access	1		1	
	Misuse	1 (2)	1		
Justice	**Access**	**9**	**1**	**8**	**—**
	Delay	**2 (11)**	**— (1)**	**2 (10)**	**—**
Labour Canada	Access	8	1	7	
National Defence	**Access**	**6**	**2**	**4**	**—**
	Misuse	**4**	**—**	**4**	**—**
	Delay	**32**	**22**	**10**	**—**
	Col/Ret/Di	**1 (43)**	**— (24)**	**1 (19)**	**—**
National Archives Canada	Access	11	4	7	
	Correction	2 (13)	(4)	2 (9)	
National Energy Board	**Access**	**1**	**—**	**1**	**—**
National Parole Board	Access	11		9	2
	Correction	1		1	
	Delay	3 (15)		3 (13)	(2)

Department	Complaint Type	Number (Total)	Justified (Total)	Dismissed (Total)	Abandoned (Total)
Privy Council Office	**Access**	**10**	**—**	**10**	**—**
	Misuse	**1 (11)**	**—**	**1 (11)**	**—**
Public Service Commission	Access	20		20	
	Correction	1 (21)		1 (21)	
Public Works	**Access**	**2**	**1**	**1**	**—**
	Misuse	**2 (4)**	**1 (2)**	**1 (2)**	**—**
Revenue Canada Customs and Excise	Access	5	2	3	
	Misuse	2		1	1
	Correction	1		1	
	Delay	2 (10)	1 (3)	1 (6)	(1)
Revenue Canada Taxation	**Access**	**12**	**2**	**10**	**—**
	Misuse	**1**	**1**	**—**	**—**
	Delay	**3**	**—**	**3**	**—**
	Col/Ret/Di	**2 (18)**	**— (3)**	**2 (15)**	**—**
RCMP	Access	71	6	64	1
	Misuse	7		7	
	Correction	7	1	6	
	Delay	13	5	8	
	Language	1		1	
	Col Ret Di	1 (100)	(12)	1 (87)	(1)
Statistics Canada	**Delay**	**1**	**—**	**1**	**—**
	Language	**1 (2)**	**—**	**1 (2)**	**—**
Solicitor General Canada	Access	4		4	
	Correction	1 (5)		1 (5)	
Supply and Services Canada	**Access**	**1**	**—**	**1**	**—**
Treasury Board	Access	1		1	
	Misuse	2 (3)		2 (3)	
Transport Canada	**Access**	**3**	**—**	**3**	**—**
	Correction	**2**	**—**	**2**	**—**
	Delay	**3 (8)**	**2 (2)**	**1 (5)**	**—**
Veterans Affairs Canada	Delay	8		8	
TOTALS		**661**	**155**	**492**	**14**

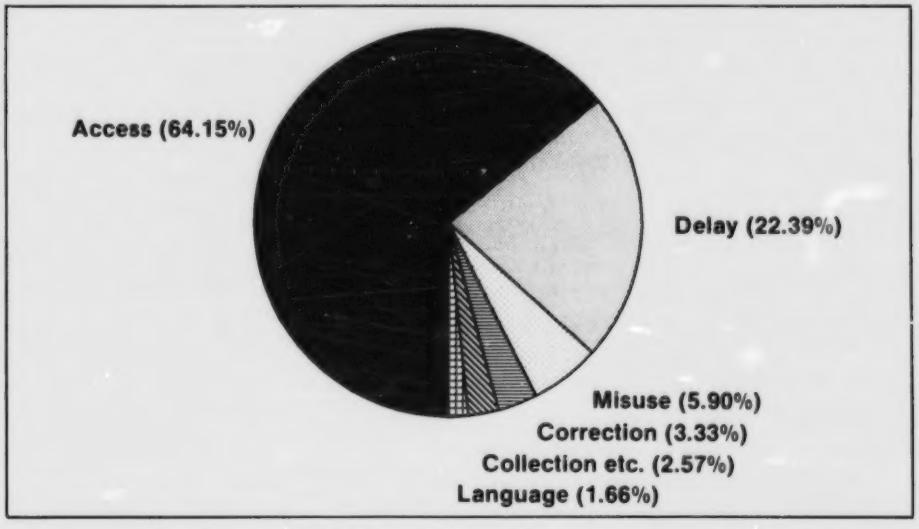
Grounds of Complaints and Investigation Results

Grounds	Abandoned	Justified	Dismissed	Total
Misuse	2	6	31	39
Access	10	54	360	424
Correction	—	2	20	22
Language	—	1	10	11
Index	—	—	—	—
Collection/ retention/disposal	1	1	15	17
Delay	1	91	56	148
TOTALS	**14**	**155**	**492**	**661**

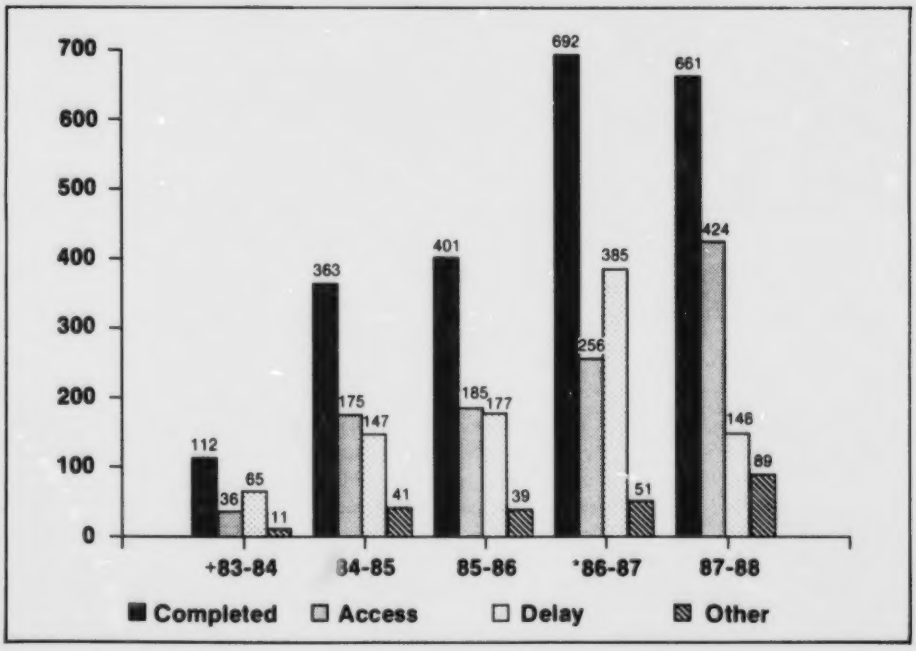
Completed complaints 1983-88



Caseload by grounds 1987-88



Completed complaints and grounds 1983-88



Disputed Status Hinders Access

A husband and wife complained that an immigration consultant hired to represent them had been refused access to their immigration files. EIC maintained that the couple did not meet the *Privacy Act* requirement that applicants be Canadian citizens or permanent residents.

Both had obtained landed immigrant status early in 1985. However, when they returned from a 1986 vacation abroad, immigration officers believed the couple had abandoned their status in Canada and so told them. The couple argued that neither had been outside the country longer than the maximum 183 days allowed and no immigration adjudicator had rescinded their status.

The privacy investigator discussed their application with EIC staff who offered to process the request under the *Access to Information Act* because the immigration consultant could apply for their information with their consent.

The consultant refused, believing that would constitute an admission that his clients were not permanent residents. While discussions continued with EIC, the immigration problem was resolved and the couple withdrew their complaint.

Contractor's Employees Protected

An Ottawa man told the Commissioner that External Affairs gave him not only the name of an agency providing the department with temporary help, but also the names of the individuals performing services.

He complained that this breached the *Privacy Act* because only the names of those signing service contracts with the government may be released because they are not "personal information". In this case the contract was with the agency and the complainant believed the individual names should be protected.

The complainant told the Commissioner that departments were not treating these applications consistently, citing several that give out only the company's name and withhold the individual employees' names. He said that the conflicting practices needed to be resolved and that the Information and Privacy Commissioners ought to provide guidance.

From his investigation the Privacy Commissioner concluded that the complaint was justified. Employees of any company providing services to the federal government on contract are not themselves government employees and, therefore, have a right to protection of their personal information.

The same applicant then asked External Affairs what security clearance was required for those idividuals' jobs. The department refused to respond because the individuals had already been identified. The applicant complained to the Information Commissioner that access was denied and this case is now before the Federal Court.

USING THE PRIVACY ACT

According to the latest Treasury Board statistics (December 31, 1987), the number of applications under the *Privacy Act* to all departments continues to climb. There were 12,013 applications during the October 1 to December 31, 1987, quarter alone — an all-time high. The total applications since July 1, 1983, when the *Privacy Act* took effect, has reached 159,835.

Processing Time

Despite the mounting number of applications, government departments appear to be more than keeping pace.

Between 1983 and 1986, only 53 per cent of the applications were processed within the 30 days allowed by the Act, 16 per cent were completed from 31 to 60 days, and 31 per cent took longer — technically a denial of access. In this fiscal year by comparison 65 per cent of the applications were handled in 30 days; 22 per cent in 60 days, and 13 per cent in more than 60 days. This steady improvement (the result of departments' increased experience, more resources and plain hard work), is another reason delay complaints are dropping.

Getting It All

Just over 64 per cent of applicants receive everything they asked for (and occasionally more). Almost 22 per cent of applicants are denied some of the information primarily because it concerns another person (47 per cent), it was supplied by a province which considers it confidential (21 per cent) or it concerns law enforcement and investigations — including RCMP information when acting as provincial police (17 per cent).

Six per cent of applicants receive nothing: one per cent either because the information is already publicly available or it is confidential Cabinet material; for the remaining five per cent information simply does not exist. For eight per cent of applicants, there is insufficient information provided to process the request, processing has proved impossible, the request has to be transferred or the request is abandoned.

These breakdowns have not changed significantly since the *Privacy Act* took effect.

Who Gets Asked

National Defence remains far ahead of all other departments in the number of applications received — it had a somewhat remarkable total of almost 73,000 by the end of 1987 — to maintain the stranglehold it has had on first place since the program began. This results largely from DND requiring its own employees to make formal applications to see their personnel files.

The next four departments in order of applications are Correctional Service Canada, 27,899; National Archives, 25,964; RCMP, 11,111; and Employment and Immigration Canada, 9,719.

Compliance Branch

"The Privacy Commissioner may, from time to time at the discretion of the Commissioner, carry out investigations...of personal information under the control of government institutions to ensure compliance..."

Section 37, Privacy Act

This year marked the first time the auditors of the compliance branch planned and completed a series of audits using the audit risk model developed last year. As the series of lost document incidents described in the 1986-87 report abated, staff was able to concentrate on auditing the compliance of four departments which management selected from those identified as "high risk".

The four, Transport Canada (TC), Correctional Service of Canada (CSC), Environment Canada (EC) and Agriculture Canada (AC), were the office's first exposure to large departments with many regional offices and full ranges of personal information banks. Previously, experience was confined to a test audit of Fisheries and Oceans and to the exempt banks of eight institutions.

The exempt bank audits proved a too-optimistic indicator of resources needed for thorough investigations. By their nature, files in exempt banks are particularly sensitive and are more uniform or homogeneous than those in other banks. They are collected according to exact parameters and are controlled centrally (though not necessarily held in a central location). There are few surprises.

This is not true of other personal information holdings. The result was a revised estimate of the depth and time required for investigations, and the development of new methodologies to handle what originally appeared to be routine audits.

Audits are conducted usually by a team of two to four investigators who visit selected headquarters units and a number of regional offices. The auditors review a random sample of files from selected banks and interview managers and staff who use and control the files.

The auditors examine:

- the department's collection, use, disclosure, retention, disposal and security of personal information;
- the adequacy of internal policies and the department's compliance with central agency policy and guidelines on personal information;
- the accuracy and completeness of the department's listing in the Personal Information Index;
- staff awareness of the *Privacy Act* and its implications for handling personal information;
- individuals' access to their personal information;
- delegation of powers by the department head.

Once the audit is completed, the auditors debrief the managers and discuss any areas of non-compliance. The department receives a draft report for discussion, then a final edition. In line with accepted audit practice, the reports address only those areas requiring correction.

The findings

Considering the differences in the four audited departments, the findings were surprisingly similar.

For example:

* apart from those in the privacy sections, few employees were aware of the impact of the *Privacy Act* on their day-to-day handling of employee or client personal information;

* with the exception of CSC, the physical security of personal information was often inadequate;

* some personal information holdings had not been identified and described in the Index;

* some information bank listings did not describe the "consistent uses" which the department routinely made of the information.

Some departments' personal information policies were found in conflict with the *Privacy Act*. Most are being remedied.

The proliferation of working copies of personnel files was another frequent observation. Although the existence of multiple copies is not addressed specifically in the *Privacy Act*, departments are required to review all copies when responding to an access request and to insure that each copy complies with the Act. The growing use of personal computers offers a new challenge in meeting this responsibility.

One final observation: each department gave auditors their complete co-operation. Most staff found the investigations interesting and treated them as an opportunity to learn more about the *Privacy Act*.

Summaries of the individual departments' reports follow.

THE AUDITS

Environment Canada

Environment Canada's three principal components, Atmospheric Environment Services (the weather office), Conservation and Protection Service and the Parks program, are spread across the country. The department collects a limited amount of personal information about the general public and what it does hold tends not to be sensitive. For example, the department has information banks containing permits issued under the *Migratory Birds Convention Act* and the *Ocean Dumping Control Act*, duck hunting and fishing licenses issued and surveys of national park visitors. The greatest part of Environment Canada's personal information holdings is that of its own employees.

The audit team visited EC offices in Sackville, New Brunswick, Dartmouth, Nova Scotia, Toronto, Ontario, Calgary, Alberta and national headquarters in Hull, Quebec.

Investigators found that:

- most Environment Canada employees knew little about the *Privacy Act*, its application and implications for their work. Internal directives were often inadequate, inaccurate and unknown;
- disposal schedules were not being applied, leading to information either being kept longer than necessary or less than the two years required by the Act;
- some personnel files were stored in insecure locations;
- personnel files about individuals on personal service contracts, volunteers, and unsolicited job applications were not described in the Personal Information Index;
- individual managers throughout the department maintain duplicate or private file systems containing personal information derived largely from personnel records, increasing the risk of unauthorized disclosure, alteration of information and denial of access;
- the *Ocean Dumping Control Act* bank contains no personal information—the files concern companies, corporations, and other federal government departments. (This bank can be removed from the Personal Information Index.)

Transport Canada

Transport Canada is one of the largest federal government departments, employing almost 22,000 persons to develop and operate a safe and efficient national transportation system. The department comprises five groups; Airports Authority, Aviation, Marine, Surface, and Policy and Coordination. The audit examined Airports Authority and Aviation and Marine groups at national headquarters and in selected regional offices.

The investigation found personal information generally well protected at Transport Canada. Employees are vigilant in preventing improper disclosure; a records management information system identified and recorded most personal information. The weaknesses found are grouped here into descriptions of personal information banks in the Personal Information Index, protection of personal information, retention and disposal, security, collection and informed use, and access.

Employee Assistance Files: One group of high risk files was identified during preparation for the investigation. These are Employee Assistance Program (EAP) files containing highly sensitive personal details. (The EAP program provides counselling and support for federal employees coping with health or behavioural problems such as alcohol abuse.) Access to these files is limited to counselling staff.

The department was understandably concerned about files being seen by outsiders — even a privacy investigator. Any unauthorized release of the information could cause irreparable harm to the individual. The office arranged with Transport Canada to have a senior privacy staff member examine a random selection of files to ensure they were properly maintained and protected. The personal identifiers were hidden.

The investigator found the files were already depersonalized, and locked in a cabinet in a locked office in a building that is inaccessible after work hours. He found no evidence of inappropriate release but made several suggestions to improve the physical security of the files.

Problems with other Transport Canada files follow.

Personal Information Index descriptions: Investigation revealed a number of defective listings including:

- the Enforcement bank (P-PU-015) contains files on enforcement activities against those holding a valid aviation document, rather than only those "not in possession" of the document;
- the Aviation Licensing Database (P-PU-005) does not indicate that its contents may be shared with the Canadian Aviation Safety Board, nor that the Medical "C" file is part of the database;
- the Vehicle Accident bank (P-SE-908), described as an employee bank, contains significant amounts of information on members of the public who have filed claims about accidents while using Transport facilities.

Protection of personal information: The investigators found that some personal information is not adequately protected from disclosure to unauthorized individuals. For example, information about aviation licence holders is available over the telephone. Lists of several employees' payroll deductions were found on individual personnel files and sensitive employee information (which belongs on a "history" file) was found on rating files.

In one regional office privacy staff found an unofficial 26-volume file containing often sensitive information on all employees, arranged in alphabetical order by name. Managers could examine the information of any employee, not just those he or she supervised.

Security was lax at some locations. Investigators found: computer disks available at night; an open concept record room with files stored on open shelves directly in front of the elevator; cleaning staff with access to licensing files, and sensitive waste thrown in regular garbage.

Retention and disposal of files: The audit team found that one information bank had no disposal schedule; two others needed review in order to send old files to National Archives for destruction or historical storage. Temporary regional files in a bank containing

accident reports are destroyed before the minimum two-year period. Although some of the material duplicates reports sent to headquarters, the files include the accident investigators' notes which should be kept.

Collection of personal information and informed use: The *Privacy Act* requires government institutions to tell individuals why they collect personal information. Such an explanation should be provided on application forms. However, forms used to issue various civil aviation licences and permits do not contain any statement of purpose. There is no indication that applicants are ever told.

Investigators found collection of what appeared to be excessive information. For example, pilots' medical examination reports ask for education data and several others require the applicants' place of birth.

Access to personal information: In one region applicants to the Aviation Licensing Database were not being given access to their medical file held in the bank unless they so specified.

Agriculture Canada

Agriculture Canada has 13,000 employees in 11 branches administering 40 different acts. Programs range from maintaining the productivity of Canada's agri-food sector to the protection of livestock and plant-life, including Canada's forests.

The audit took place in Moncton, New Brunswick, Calgary, Alberta, and Ottawa-Hull headquarters.

Protection of personal information: Investigators found a number of working personnel files in regional offices containing sensitive personal details. Other files contained unnecessary information about third parties. In several locations, personal information was unlocked in open offices. In one case, the open files concerned investigations of alleged wrongdoings.

Working personnel files are common in regional offices where they are kept for routine management purposes. Working files do not necessarily contravene the *Privacy Act* providing that they are exact duplicates of official files; their use is restricted to those with a need to know, and they are reviewed when an employee submits a privacy request.

Improper disclosure: Agriculture Canada signed a 1985 Memorandum of Agreement with Canada Customs and the RCMP to provide investigation reports to an automated RCMP database. These three agencies, police forces and the United States Customs Service share the information.

Investigators considered that, with few exceptions, the disclosures were unrelated to the original collection purpose and suggested the department stop releasing information unless it conforms to the *Privacy Act*. The department should respond only to written requests from investigative bodies such as the RCMP, keeping records of all disclosures for the Privacy Commissioner's examination.

Awareness of the Privacy Act: Few employees were familiar with the Act. The result can be improper handling

of personal information, for example, keeping indefinitely conflict-of-interest reports about former employees. The department agreed to delete old information on one system and to modify its new system to include file destruction dates. The difficulty with the agreement with Customs and the RCMP, described above, stemmed from lack of knowledge of the Act.

Correctional Service Canada

Correctional Service Canada consists of the Penitentiary Service, responsible for inmate custody and care, and National Parole Service which supervises those freed on parole or mandatory supervision.

Given the demands of their jobs, employees consider security, confidentiality, and protection of personal information a routine part of their work.

However, there were areas where improvements could be made.

Personal Information Index descriptions: Investigators found inaccurate or incomplete bank descriptions in the Index or, in some cases, the purpose for the collection was unclear. There were files containing information services inquiries, ministerial inquiries, administrative inquiries, inmate transfer files and offender administrative case files — all of which are collections of personal information but not described in the Index.

In addition, there were 12 series of files containing personal information not listed in the Index, thus effectively removing the information from access and leaving the public unaware of the extent of the collection or its purpose. It can also mean these files are not held for the minimum two years nor reviewed for regular destruction.

Protection of personal information: The investigators found that employees in the Ontario and Quebec regions can only review their personnel file through a request to their supervisor and in the supervisor's presence. Some Ontario and Quebec offices lack policies for secure disposal of legible computer and typewriter ribbons.

At national headquarters, sensitive pardon records were found on open shelving in a basement storage area. They were available to anyone with access to the room.

Access rights: Inmates requesting access to the Psychology bank (CPS/P-PU-070) in the Ontario Region are not receiving their raw test data. Psychology staff at the Ontario Regional Psychiatry Centre and Joyceville Institution routinely withhold the scores before sending the files to headquarters, without the knowlege of the department's privacy coordinator. Applicants are not told of the omission, nor of their right to complain to the Privacy Commissioner.

Use and Disclosure Code: The problems the Commissioner's office has encountered with CSC's use and disclosure code are discussed in detail on page 16.

Notifying the Commissioner

One of the tenets of the *Privacy Act* is its protection against release of individuals' personal information. But as with most rules, there are exceptions. For example, personal data may be released "in the public interest", to comply with another act of Parliament or a warrant or subpoena, to specified investigative agencies, and to the National Archives for storage.

But government departments must notify the Privacy Commissioner when they decide to so release personal information or for any new use "consistent" with the purpose for which it was originally collected. This notice gives the Commissioner an opportunity to object to those releases he considers improper and to advise the individuals if he considers it necessary.

The Commissioner received the following such notifications this year:

Statistics Canada: confirmation of several persons' birthplaces or ages to relatives to apply for pension benefits or to confirm citizenship for Canadian or U.S. passports.

— refused release of information about individuals, born in East bloc countries, who died in Canada intestate.

Indian Affairs and Northern Development: confirmation of deceased man's Indian status to help daughter obtain Indian status.

Justice: release of lawyer's opinion concerning Canadian government funding of the Allan Memorial Institute. The department released the opinion (which contained personal information about three men), after obtaining the subjects' consent;

— release of two letters to a law society for background in a complaint of misconduct against a departmental lawyer.

National Defence: release of treating physician's affidavit to wife of man in coma, to permit her to manage family's financial affairs.

Royal Canadian Mounted Police: release of RCMP report on death of serving member to his widow to pursue pension claim.

Veterans' Affairs: release of deceased veteran's medical records to his daughter's doctor to investigate possibility of inherited disease.

— release of deceased's medical records to son to help treatment of suspected hereditary conditions.

National Parole Board: release of parole board decision and reasons for decision to an MP querying allegations of political interference in the decision.

Solicitor General: release to House of Commons of report, prompted by McDonald Commission findings, recommending how Canada should fulfil outstanding obligations to Warren Hart.

Secretary of State: release of woman's Canadian citizenship data so Japanese authorities could enforce a Canadian child custody order.

— confirmation of dates on which 13 individuals granted Canadian citizenship to determine eligibility for Order of Canada. Three nominees' information could not be found.

Spreading the Word

The Privacy Commissioner and his staff continued to stump the country for privacy. The Commissioner spoke to, among others, Canadian Club audiences in Moose Jaw, Saskatchewan, and London, Ontario. He discussed privacy auditing with the Institute of Internal Auditors; privacy codes with the Canadian Direct Marketing Association; privacy and human rights with the Canadian Law and Society Conference; monitoring and surveillance at the annual conference of international data protectors in Quebec City and the implications of privacy legislation on information management at the national records management conference in Melbourne, Australia.

Since privacy is particularly relevant to statistical collection (statisticians rely heavily on manipulation of administrative records), the Commissioner addressed Statistics Canada's management conference as well as international statisticians in both Ottawa and Stockholm. In addition, the Commissioner was interviewed by the media and he participated in meetings with newspaper editorial boards.

His staff briefed candidates on the senior management courses at the federal government's executive training centre, and spoke to post secondary classes, federal employee seminars, and the annual meetings of the Canadian Information Processing Society and the Canadian Society for Information Science.

Inquiries

The year's 1,248 inquiries ranged from whether a jewellery store owner could require employees to inspect one another's handbags and parcels before leaving work, to a call from a utility company wondering whether it could use Social Insurance Numbers to locate customers who moved, leaving unpaid accounts. The jewellery store is not under the jurisdiction of the *Privacy Act* and the utility company can use SINs, but having clients' numbers won't give it access to the federal government's data banks to find their new addresses.

Just over 14 per cent of the inquiries were applications for personal files which were redirected to the departments holding the information. These particular inquiries are reminders that many individuals continue to believe that Ottawa has one large file about them — a perception the Commissioner is happy to dispel.

Almost 50 per cent of callers ask what the Act is, how they can see their personal information, or want some clarification about the law.

Nearly six per cent called about the potential invasion of privacy from such federal programs as Statistics Canada surveys and the government's new conflict of interest and security clearance policies for its employees.

About ten per cent of the calls, while related to privacy, were not in the federal jurisdiction. The Commissioner's office is now able to refer such Ontario callers to their new Information and Privacy Commissioner, although he too is unable to deal with complaints involving private businesses.

Just over seven per cent of the calls were unrelated, including requests for leads to track down natural parents and a call wondering why a local housing authority wanted an applicant's tax return.

Queries and complaints about Social Insurance Number incidents increased to more than 15 per cent of the total inquiries, partly reflecting the Commissioner's comments in his last annual report, and partly because of the federal government's promise to tighten its own collection and use of the numbers. Callers objected to such things as having to produce the number to vote in a municipal election, join a seniors' travel club and, in one novel instance, to having it programmed into their employer's photocopier to restrict their access to the machine as well as to monitor use and cost.

The office receptionist referred an astonishing 5,756 calls to either the federal government's central switchboard or, more recently, Reference Canada. The majority of these completely unrelated calls are prompted by the national toll-free number listed under "Information Commissioner" (with whom the Privacy Commissioner shares offices) in the blue pages of municipal telephone directories. Callers believe the office is the new Information Canada.

Corporate Management

Corporate Management provides both the Information and Privacy Commissioners with financial, personnel, administrative, data processing and library services.

Finance

The Offices' total resources approved by Parliament for the 1987-88 fiscal year were $3,922,000 and 58 person years, an increase of approximately $3,000 over the 1986-87 expenditures. Personnel costs of $2,970,000 and professional and special services expenditures of $512,000 accounted for more than 89 per cent of expenditures. The remaining $440,000 covered all other expenses.

Personnel

Staff increased by five during the fiscal year, to a total of 58 on March 31, 1988. There were 21 staffing actions during the year, including one appointment to a senior management position: Executive Director, Office of the Privacy Commissioner.

Administration

During this past year, space was acquired on the third and fourth floors, Tower B, Place de Ville. This space is presently being fitted-up and will be ready for occupancy by the summer.

The following are the Offices' expenditures for the period April 1, 1987 to March 31, 1988

	Information	Privacy	Administration	Total
Salaries	$ 968,062	$1,121,001	$ 483,768	$2,572,831
Employee Benefit plan contributions	159,200	149,640	88,160	397,000
Transportation and Communications	25,028	59,518	98,698	183,244
Information	47,258	50,028	558	97,844
Professional and special services	412,534	72,754	26,411	511,699
Rentals	76	727	11,172	11,975
Purchases repair and maintenance	222	1,163	1,225	2,610
Utilities, material and supplies	4,191	11,171	27,778	43,140
Construction and equipment acquisition	32,494	33,141	16,344	81,979
All other	79	1,245	177	1,501
TOTAL	**$1,649,144**	**$1,500,388**	**$ 754,291**	**$3,903,823**

Data Processing

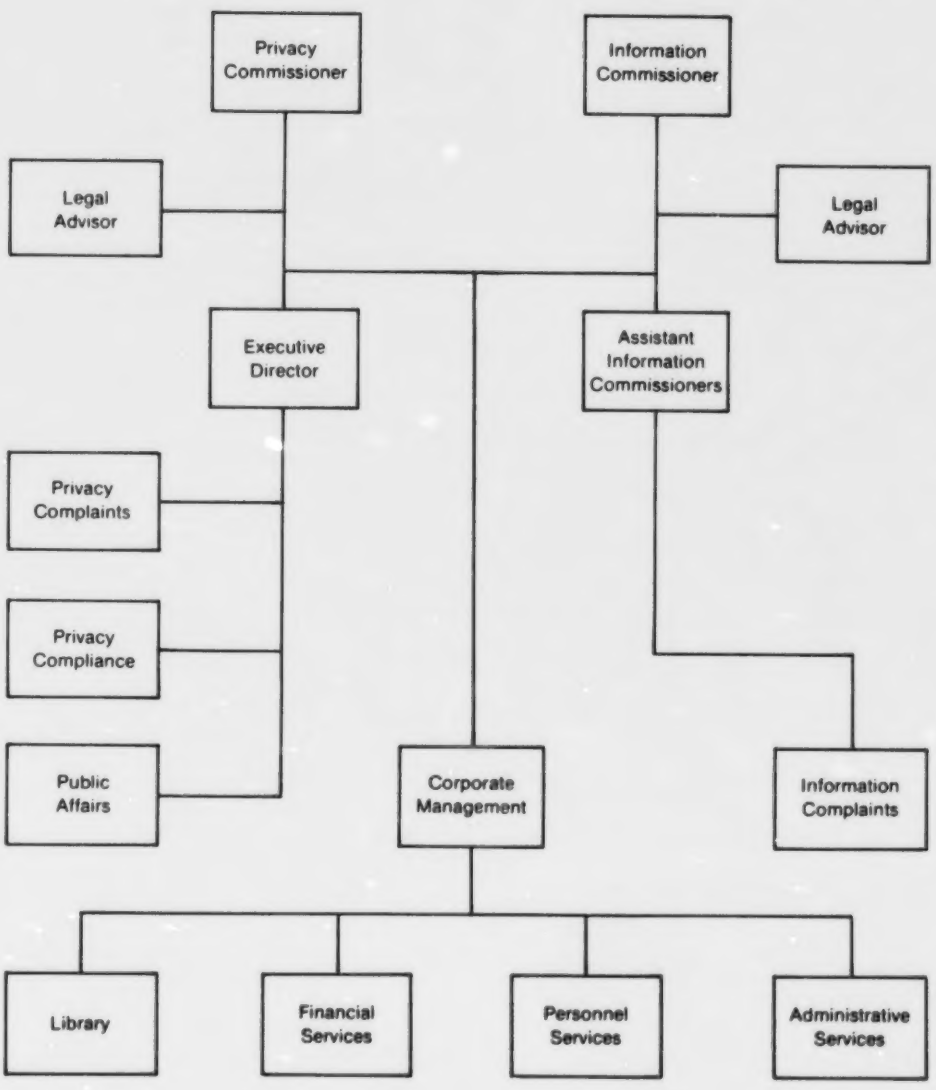
Computerization of the Offices has increased in most areas and as a result, staff has become more adept at using data processing equipment in their daily tasks. A larger volume of information has been processed and computer stored.

Library

The library obtains and disseminates information for both Commissioners' offices. To assist in this function, subscriptions to several automated bibliographic and full text data bases are maintained. An interlibrary loan service is also available to the users. Freedom of information, protection of privacy and the Ombudsman function are the main subject areas of the library's collection of approximately 3000 items. The public is invited to consult the library for reference and research. Last year 25 visitors were welcomed, 630 reference questions were answered and 450 items were added to our collection.

Appendix I

Offices of the
Information and Privacy
Commissioners of Canada



Appendix II

Government Institutions Covered by the Act

Advisory Council on the Status of Women

Agricultural Products Board

Agricultural Stabilization Board

Agriculture Canada

Atlantic Development Council

Atlantic Pilotage Authority

Atomic Energy Control Board

Bank of Canada

Bilingual Districts Advisory Board

Board of Trustees of the Queen Elizabeth II Canadian Fund to Aid in Research on the Diseases of Children

Bureau of Pension Advocates

Canada Council

Canada Deposit Insurance Corporation

Canada Employment and Immigration Commission

Canada Labour Relations Board

Canada Lands Company Limited

Canada Mortgage and Housing Corporation

Canada-Newfoundland Offshore Petroleum Board

Canada Ports Corporation

Canada Post Corporation

Canadian Aviation Safety Board

Canadian Centre for Occupational Health and Safety

Canadian Commercial Corporation

Canadian Cultural Property Export Review Board

Canadian Dairy Commission

Canadian Film Development Corporation

Canadian Government Specifications Board

Canadian Grain Commission

Canadian Human Rights Commission

Canadian Import Tribunal

Canadian Institute for International Peace and Security

Canadian International Development Agency

Canadian Livestock Feed Board

Canadian Patents and Development Limited

Canadian Penitentiary Service

Canadian Pension Commission

Canadian Radio-televison and Telecommunications Commission

Canadian Saltfish Corporation

Canadian Security Intelligence Service

Canadian Unity Information Office

The Canadian Wheat Board

Communications, Department of

Consumer and Corporate Affairs Canada

Defence Construction (1951) Limited

The Director of Soldier Settlement

The Director, The Veterans' Land Act

Economic Council of Canada

Employment and Immigration Canada

Energy, Mines and Resources Canada

Energy Supplies Allocation Board

Environment Canada

Export Development Corporation

External Affairs Canada

Farm Credit Corporation

Federal Business Development Bank

Federal Mortage Exchange Corporation

Federal-Provincial Relations Office

Finance, Department of

Fisheries and Oceans Canada

Fisheries Prices Support Board

The Fisheries Research Board of Canada

Freshwater Fish Marketing Corporation

Grain Transportation Agency Administrator

Great Lakes Pilotage Authority, Ltd.

Health and Welfare Canada

Historic Sites and Monuments Board of Canada

Immigration Appeal Board

Indian and Northern Affairs Canada

International Development Research Centre

Investment Canada (formerly Foreign Investment Review Agency)

Jacques Cartier and Champlain Bridges Incorporated

Justice Canada

Labour Canada

Laurentian Pilotage Authority

Law Reform Commission of Canada

Medical Research Council

Merchant Seamen Compensation Board

Metric Commission

National Archives of Canada

National Arts Centre Corporation

The National Battlefields Commission

National Capital Commission

National Defence

National Design Council

National Energy Board

National Farm Products Marketing Council

National Film Board

National Library

National Museums of Canada

National Parole Board

National Parole Service

National Research Council of Canada

National Transportation Agency (formerly Canadian Transport Commission)

Natural Sciences and Engineering Research Council

Northern Canada Power Commission

Northern Pipeline Agency

Northwest Territories Water Board

Office of the Auditor General

Office of the Chief Electoral Officer

Office of the Commissioner of Official Languages

Office of the Comptroller General

Office of the Coordinator, Status of Women

Office of the Correctional Investigator

Office of the Custodian of Enemy Property

Office of the Inspector General of the Canadian Security Intelligence Service

Office of the Superintendant of Financial Institutions Canada

Pacific Pilotage Authority

Pension Appeals Board

Pension Review Board

Petroleum Compensation Board

Petroleum Monitoring Agency

Prairie Farm Assistance Administration

Prairie Farm Rehabilitation Administration

Privy Council Office

Public Service Commission

Public Service Staff Relations Board

Public Works Canada

Regional Development Incentives Board

Regional Industrial Expansion

Revenue Canada

Royal Canadian Mint

Royal Canadian Mounted Police

Royal Canadian Mounted Police External Review Committee

RCMP Public Complaints Commissioner

The St. Lawrence Seaway Authority

Science and Technology Canada

Science Council of Canada

The Seaway International Bridge Corporation, Ltd.

Secretary of State

Security Intelligence Review Committee

Social Development, Ministry of State for

Social Sciences and Humanities Research Council

Solicitor General Canada

Standards Council of Canada

Statistics Canada

Statute Revision Commission

Supply and Services Canada

Tariff Board

Tax Review Board

Textile and Clothing Board

Transport Canada

Treasury Board Secretariat

Veterans' Affairs Canada

War Veterans Allowance Board

Yukon Territory Water Board

Rapport annuel du Commissaire à la protection de la vie privée 1987-88

Le Commissaire à la protection de la vie privée du Canada
112, rue Kent,
Ottawa (Ontario)
K1A 1H3

(613) 995-2410
1-800-267-0411

Le standard téléphonique est ouvert de
7 heures 30 à 18 heures, heure d'Ottawa

© Ministre des Approvisionnements et Services Canada 1988

N° de cat. IP30-1/1988

ISBN 0-662-55287-3

"Les seuls renseignements personnels que peut recueillir une institution fédérale sont ceux qui ont un lien direct avec ses programmes ou ses activités . . . ".

"Une institution fédérale est tenue de recueillir auprès de l'individu lui-même, chaque fois que possible, les renseignements personnels . . . le concernant . . . ".

" . . . est tenue d'informer l'individu . . . des fins auxquelles ils (les renseignements personnels) sont destinés".

" . . . est tenue de veiller, dans la mesure du possible, à ce que les renseignements personnels . . . soient à jour, exacts et complets".

"À défaut du consentement de l'individu concerné, les renseignements personnels relevant d'une institution fédérale ne peuvent servir à celle-ci :

a) qu'aux fins auxquelles ils ont été recueillis ou préparés . . . "

(ou conformément aux exceptions précises énoncées à l'article 8)

La *Loi sur la protection des renseignements personnels.*

L'honorable Guy Charbonneau
Président
Sénat
Ottawa

le 30 juin 1988

Monsieur Charbonneau,

J'ai l'honneur de soumettre mon rapport annuel au Parlement. Ce rapport couvre la période allant du 1er avril 1987 au 31 mars 1988.

Veuillez agréer l'expression de mes sentiments respectueux.

John W. Grace

Le Commissaire à la protection de la vie privée,
John W. Grace

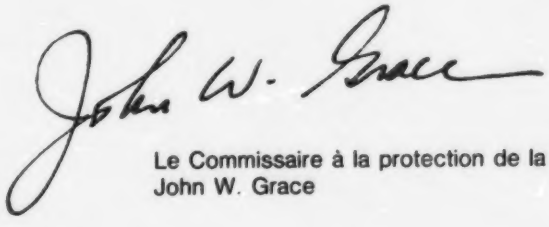
L'honorable John A. Fraser, c.p., c.r., député
Président
Chambre des communes
Ottawa

le 30 juin 1988

Monsieur Fraser,

J'ai l'honneur de soumettre mon rapport annuel au Parlement. Ce rapport couvre la période allant du 1er avril 1987 au 31 mars 1988.

Veuillez agréer l'expression de mes sentiments respectueux.



Le Commissaire à la protection de la vie privée,
John W. Grace

Table des matières

Mandat ... 1
Cinq ans déjà ... 2
Les problèmes — anciens et nouveaux ... 14
  Le couplage des données et le NAS ... 14
  Usage compatibles ... 16
  Protection de la vie privée des détenus en libération conditionnelle et internés ... 16
  La protection de la vie privée au travail ... 18
Direction des plaintes ... 23
  Plaintes ... 31
Direction de l'observation ... 40
  Les vérifications ... 41
  Environnement Canada ... 41
  Transports Canada ... 42
  Agriculture Canada ... 44
  Le Service correctionnel du Canada ... 45
Aviser le Commissaire ... 47
Faites passer ... 49
Les demandes de renseignements ... 50
Gestion intégrée ... 51
Annexe I ... 53
Annexe II ... 54

Mandat

La *Loi sur la protection des renseignements personnels* donne aux individus accès à leurs renseignements personnels détenus par le gouvernement fédéral; protège la vie privée des individus en restreignant le nombre des personnes qui peuvent consulter les renseignements; et donne aux individus un certain contrôle sur la collecte et l'usage des renseignements par le gouvernement.

La Loi énonce les principes des pratiques équitables en matière d'information qui exigent que le gouvernement :

- ne collecte que les renseignements dont il a besoin pour exécuter ses programmes;
- recueille les renseignements directement auprès de l'individu concerné, dans la mesure du possible;
- informe l'individu des fins auxquelles ils sont destinés;
- conserve les renseignements suffisamment longtemps pour en assurer l'accès aux individus; et
- veille « dans la mesure du possible » à ce que les renseignements personnels soient exacts et complets.

Les citoyens canadiens ou les résidents permanents peuvent déposer une plainte auprès du Commissaire à la protection de la vie privée si :

- ils se sont vus refuser une partie quelconque des renseignements;
- le droit de demander la correction de certains des renseignements contenus dans le fichier ou de les annoter leur est refusé;
- le ministère prend plus des 30 jours initiaux ou des 60 jours maximums pour fournir les renseignements;
- la description du contenu des fichiers de renseignements donnée dans le Répertoire des renseignements personnels est incorrecte à un quelconque égard;
- la liste donnée dans le Répertoire pour chaque ministère ne décrit pas tous les usages qui sont faits des renseignements personnels;
- une institution recueille, conserve ou élimine des renseignements personnels d'une manière qui contrevient à la *Loi sur la protection des renseignements personnels*.

Les enquêteurs du Commissaire à la protection de la vie privée examinent tous les fichiers (y compris ceux qui figurent dans les banques inconsultables), à l'exception des renseignements confidentiels du Conseil privé de la Reine, pour s'assurer que les institutions fédérales se conforment à la Loi.

La Loi confère également au Commissaire à la protection de la vie privée le pouvoir de vérifier la façon dont les institutions fédérales recueillent, utilisent et éliminent les renseignements personnels, sans devoir attendre qu'une plainte soit déposée.

Cinq ans déjà!

Voilà déjà cinq ans que nous bénéficions de la *Loi sur la protection des renseignements personnels*, cinq ans que nous rendons compte au Parlement (et au pays) de l'application de sa législation; cinq ans d'activité fébrile et de mises en garde concernant les risques que font peser les nouvelles technologies de l'information — généralement employées dans une bonne intention au nom de l'efficacité — sur des valeurs humaines précieuses et vulnérables.

Ces années représentent peu dans la vie d'une loi. Elles n'ont pas été suffisantes d'ailleurs pour produire des résultats dans un appareil aussi complexe et rigide que l'administration fédérale. On doit pourtant conclure d'ores et déjà que le bien-fondé de la *Loi sur la protection des renseignements personnels* a effacé le scepticisme initial (souvent bien compréhensible). Ce jugement ne vient pas d'un ardent partisan comme le Commissaire à la protection de la vie privée, mais bien du gouvernement dans la réponse qu'il a faite pendant l'année au rapport très approfondi et très encourageant d'un comité parlementaire sur la *Loi*.

Aujourd'hui, on ne se demande plus s'il faut légiférer pour protéger les renseignements personnels, mais si la portée de la *Loi* et son mandat suffisent compte tenu des menaces existantes et des défis à relever.

Il paraît impensable de nos jours qu'un pays démocratique ne surveille pas l'emploi des renseignements personnels toujours plus nombreux que son gouvernement demande aux particuliers. Les nouveaux risques d'atteinte à la vie privée sont si graves, et si difficiles à prévoir, qu'aucun code ne pourrait à lui seul les prévoir tous.

Voyez ce qui est arrivé à Robert Bork pendant qu'il comparaissait devant le Sénat en vue d'une nomination comme juge de la Cour suprême des États-Unis. Un journal de Washington a obtenu et publié une liste des films que M. Bork avait loués dans un magasin de vidéo. Mais avant cette intrusion scandaleuse dans la vie privée, qui avait pensé à protéger l'intimité des clients des magasins de vidéo? (Un sénateur américain a été tellement dégoûté par le manque d'éthique des journalistes qu'il a apporté au comité une copie de sa propre fiche de location pour montrer les risques de fausse interprétation. Il avait loué une cassette que le magasin avait désignée « Cat on a Hot », alors qu'il s'agissait d'un code pour « Cat on a Hot Tin Roof ».)

Tout de suite après cette intrusion caractérisée dans la vie privée, certains États américains ont proposé de légiférer contre des actions aussi ignobles.

Mais que devra empêcher la nouvelle loi? D'où viendra la prochaine violation effrayante du droit à la vie privée? Faut-il craindre que les bibliothèques publiques ne communiquent aux enquêteurs ou aux journalistes des listes d'ouvrages empruntés? Nous espérons bien que non. Pourtant, aussi bien dans un magasin de vidéo que dans une bibliothèque, dans les bureaux du personnel ou de crédit, un employé n'a qu'à appuyer sur un bouton pour obtenir des renseignements personnels qui causeront du tort à quelqu'un, le diffameront ou simplement amuseront la galerie.

La prolifération des tests plus ou moins fiables est un autre exemple qui montre à quel point il peut être difficile de ne pas se laisser distancer par la technologie (et parfois d'éviter l'hystérie) dans le domaine de la protection de la vie privée.

Les anciennes évaluations personnelles de qualification, de caractère et d'expérience font place à la science ou à la pseudo-science. Un spécialiste américain de la protection de la vie privée, Robert Ellis Smith, a noté que dans son pays les employés sont de plus en plus souvent contraints à donner leurs empreintes digitales, à se soumettre aux détecteurs de mensonge, à des analyses d'urine, à des tests psychologiques, des examens sanguins, des vérifications informatisées de casier judiciaire, des études graphologiques, et leur recrutement peut même parfois dépendre de . . . l'astrologie.

William Safire a écrit dans le *New York Times* :

« Nous nous espionnons mutuellement. Demain au bureau, vous voyez-vous donner des échantillons de sang et d'urine, passer au polygraphe de la maison, vider vos poches et passer sous quelque nouveau fluoroscope? Vous êtes contre? Pourquoi? Auriez-vous quelque chose à cacher? »

Nous n'avons rien à cacher, mais tout à perdre au chapitre de la dignité et de l'intimité.

John Shattuck, qui enseigne la législation de la protection de la vie privée à Harvard et est vice-président de cette université, a dit que les pratiques et les systèmes nouveaux qui envahissent les secteurs autrefois exclusivement du domaine privé « échappent par définition à la réglementation ». Les technologies modernes ne sont pas visées par la législation traditionnelle de la vie privée, déclare-t-il « parce qu'il n'y a pas de loi, que la loi est périmée, ou qu'on a tout simplement décidé de ne pas l'appliquer ».

Cette situation ne satisfait personne, ni les libéraux ni les conservateurs, ni la gauche ni la droite.

Au Canada, on n'emploie peut-être pas encore les tests prétendument objectifs et impersonnels qui sont devenus monnaie courante ailleurs, mais si nous n'y prenons pas garde, c'est peut-être ce qui nous attend demain.

Une meilleure protection

On se console comme on peut. Après cinq ans d'existence, la *Loi sur la protection des renseignements personnels* est appliquée avec de plus en plus de rigueur et de réceptivité. Même si l'application de la Loi n'est pas uniforme, le public a de plus en plus de garanties (et non le contraire) que les renseignements confiés — souvent par la force des choses — au gouvernement fédéral serviront exclusivement aux fins annoncées et ne seront vus que par des personnes autorisées ou qui en ont besoin.

Il est primordial de défendre ces principes et de les faire respecter. Car ceux qui savent, utilisent leurs connaissances (un truisme comme l'a signalé *The Economist)* comme l'ont fait « de nombreuses personnes tout au long des siècles, depuis Ève tentée au Jardin d'Eden jusqu'à Ivan Boesky, à New York » ou, plus près de nous, un ministre du cabinet de la Nouvelle-Écosse.

La grande raison d'être des lois sur la protection de la vie privée est de protéger les personnes. Les législateurs les ont formulées dans une bonne intention, parce qu'ils étaient persuadés qu'il fallait protéger leurs électeurs de tout emploi abusif par l'État des renseignements personnels les concernant.

Les gouvernements doivent pourtant reconnaître que ces lois les protègent efficacement eux aussi, même si elles sont parfois un inconvénient ou un obstacle. Le public donnera plus volontiers des renseignements personnels exacts au gouvernement, requis par la loi (recensement ou déclaration d'impôt) ou fournis volontairement (sondage), s'il sait que ceux-ci sont protégés par les principes qui régissent la *Loi sur la protection des renseignements personnels*.

En outre, les pays qui ont légiféré dans ce domaine hésitent de plus en plus à laisser les renseignements concernant leurs ressortissants circuler librement vers des pays dépourvus de législation similaire. L'existence de « paradis de données » outre-mer mettrait en danger la souveraineté, l'économie et le droit à la vie privée.

Les bonnes intentions n'expliquent donc pas à elles seules que des pays aussi différents que les Pays-Bas, la Grèce, l'Irlande, la Finlande et le Japon aient déposé cette année des projets de loi très comparables à la loi en vigueur au Canada depuis cinq ans (huit ans si l'on compte la IV[e] Partie de la *Loi canadienne sur les droits de la personne*).

Pour une raison ou une autre, l'amélioration de la protection des renseignements personnels figure dans plusieurs ordres du jour nationaux, peut-être au bas de la liste, mais au moins à la rubrique « autres affaires ».

Au Canada, l'an dernier, la grande nouvelle en matière de protection des renseignements personnels n'a pas été un scandale fracassant ou une perte rocambolesque de documents, Dieu merci, l'épidémie semble endiguée.

Non, l'événement majeur, et c'est rassurant, a été l'engagement du gouvernement d'accepter les recommandations clés du rapport du Comité de la Justice et du Solliciteur général, *Une question à deux volets : Comment améliorer le droit d'accès à l'information tout en renforçant les mesures de protection des renseignements personnels*, qui a fait suite à son étude de la *Loi sur la protection des renseignements personnels* et de la *Loi sur l'accès à l'information*.

« Le gouvernement reconnaît que l'on pourrait modifier la *Loi sur la protection des renseignements personnels* afin de la rendre plus efficace sur le plan de la protection des données. Sa modification lui permettrait de demeurer à l'avant-garde pour ce qui est des questions concernant la protection des renseignements personnels et de l'établissement de normes en vue d'exercer un contrôle efficace sur la collecte, l'utilisation et la divulgation de renseignements par les institutions gouvernementales. »

C'est écrit noir sur blanc dans la réponse du gouvernement aux recommandations du Comité, intitulée *Les prochaines étapes*. Un commissaire à la protection de la vie privée n'aurait pas fait mieux.

Le coup d'envoi est donné

Mais nous nous félicitons surtout de voir le coup d'envoi donné : des changements importants sont apparus, dont la nouvelle politique sur le couplage des données que l'on est à mettre en place et qui est capitale. Le Canada possèdera donc un code de couplage des données qui pourrait bien être le plus sévère et, du point de vue du défenseur de la protection des renseignements personnels, le plus perfectionné de tous les pays.

Il y a cinq ans, les expressions « interconnexion des ordinateurs » ou « couplage des données », si même elles existaient, étaient probablement associées à un service informatisé ultramoderne de rencontres pour cœurs esseulés. C'est en fait une technique qui, si elle n'était pas réglementée, constituerait une menace orwellienne qu'Orwell lui-même n'aurait pu imaginer. L'emploi envahissant et systématique de l'informatique pour recueillir, stocker et comparer les renseignements personnels à tort ou à raison réduit les personnes à des objets, ramène les valeurs humaines à la seule efficacité.

Il serait téméraire de prétendre que le danger est conjuré. Mais, bien appliquée, la nouvelle politique de couplage des données permet raisonnablement d'espérer que l'ère du citoyen transparent est au moins reportée à plus tard.

Peut-être est-il vain, et passéiste, d'affirmer qu'on n'autorisera jamais le couplage, car l'informatique a des avantages indéniables. Il y a quatre ans, le Commissaire à la protection de la vie privée avait axé son rapport sur la nécessité de veiller à « l'existence de lignes de conduite adéquates pour empêcher les violations de la vie privée personnelle ». Selon ce rapport, le couplage des données effectué sans le consentement des intéressés et à d'autres fins que celles qui avaient été invoquées est au moins implicitement interdit par la *Loi sur la protection des renseignements personnels*.

Nous avons été rassurés de constater dans *Les prochaines étapes* que le gouvernement croit que « les dispositions actuelles de la *Loi sur la protection des renseignements personnels* constituent une autorisation suffisante pour réglementer le couplage et l'interconnexion des données ». Reste donc à garantir l'efficacité de la réglementation.

Si l'esprit et la lettre de la nouvelle politique concernant le couplage et l'interconnexion des données sont respectés, les Canadiens auront pour la première fois une assurance raisonnable que leur vie privée ne sera pas systématiquement violée quand les technocrates des énormes banques de données du gouvernement fédéral mettront leurs ordinateurs en route. Le fait est qu'on a coupé l'herbe sous les pieds de certains informaticiens.

Même si elle n'avait servi à rien d'autre cette année — ou depuis cinq ans — la *Loi* aurait prouvé son utilité en étant l'instrument de réglementation du couplage. On n'insistera jamais assez sur l'importance de ce rôle.

Il y a deux ans, le professeur Kenneth C. Laudon, autorité américaine en matière de systèmes informatisés, a écrit un ouvrage appelé *Dossier Society*, cette société étant le revers de la médaille de l'économie d'information. Selon lui, la force de la nouvelle technologie réside dans « sa faculté de faire circuler efficacement les renseignements à travers les frontières qui séparent les organisations et de les combiner avec les données de programmes et de fichiers très différents ».

Voici comment le professeur Laudon décrit les grands traits de la « société fichée » du point de vue de l'individu :

« . . . Les décisions prises à notre sujet comme citoyens, employés, consommateurs, débiteurs et demandeurs se font de moins en moins lors de rencontres personnelles, en fonction de nos dires ou de notre expérience. Tout repose sur des renseignements pris dans des réseaux nationaux, et interprétés par des bureaucrates et des commis qui ne sont pas sur place . . . Ces décisions sont fondées sur un 'profil informatisé' constitué à partir de plusieurs fichiers. »

La *Loi sur la protection des renseignements personnels* est le seul outil que possède le Canada pour réglementer cet échange de renseignements, le seul frein à une surveillance informatique des individus par l'administration fédérale. Et, comme nous l'avons dit dans des rapports antérieurs, il y avait toujours jusqu'ici de bonnes raisons pour agir de cette façon : retracer ceux qui refusent de payer les pensions alimentaires imposées par les tribunaux, débusquer les tricheurs du bien-être social et les débiteurs, créer des systèmes centralisés de renseignements pour la police.

C'est justement le bien-fondé de la cause qui rend le couplage si intéressant, et si difficile à arrêter. Le professeur Laudon soutient pourtant qu'un couplage illimité confère à un gouvernement central une « concentration de pouvoir » sans précédent sur ses citoyens en temps de paix et qu'elle est inconstitutionnelle. Chaque fois que des bureaucrates se réunissent pour créer des réseaux nationaux d'information, « on assiste à une mini-conférence constitutionnelle » conclut-il avec inquiétude. Bien que ce soit un peu exagéré, les effets de la centralisation informatique et des échanges de renseignements personnels à l'échelle nationale pourraient être beaucoup plus graves qu'on ne le croit dans ce pays.

Voilà pourquoi l'engagement du gouvernement de surveiller ses ordinateurs aux termes de la *Loi sur la protection des renseignements personnels* est la meilleure nouvelle de l'année ou peut-être des dernières années. Il incombe maintenant au Commissaire de bien surveiller la politique. Il ne faut pas attendre l'avènement de la société fichée pour agir.

Mon NAS? Non merci!

Autre bonne nouvelle : le gouvernement a officiellement reconnu que les Canadiens ne veulent pas que le numéro d'assurance sociale (NAS) devienne un numéro d'identification universel. Dans *Les prochaines étapes*, il s'engage à « prévoir qu'il ne peut être refusé à quiconque un droit, un avantage ou un privilège et qu'il ne peut être imposé de peine » à une personne qui refuse de fournir à une institution fédérale son NAS, à moins que la communication en soit exigée aux fins de la divulgation des programmes et des activités susmentionnés ».

Cette politique fait fi de notre recommandation de l'année dernière selon laquelle aucun organisme, aucun gouvernement ou autre ne devrait refuser des biens, des services ou des avantages à quelqu'un qui aurait refusé de fournir son NAS — sauf, évidemment, si c'était expressément requis par la loi. C'est pourtant un bon début. Les obstacles juridiques à une attaque en règle contre la tyrannie du NAS sont considérables.

Même dans cette situation, on sent poindre la main de fer sous un gant de velours. Le gouvernement a déclaré que si les secteurs public et privé ne limitent pas l'emploi du NAS, il « examinera l'adoption de mesures législatives ... y compris, au besoin, des modifications du *Code criminel* pour qu'il soit interdit de demander un NAS, sauf dans les cas autorisés par la loi ».

En donnant un sérieux coup de frein à l'utilisation abusive du NAS dans ses propres services, le gouvernement acquiert une autorité morale pour sermonner les autres instances publiques et le secteur privé.

Élargissement du mandat du Commissaire

La troisième bonne nouvelle à annoncer est la promesse d'élargir le mandat de la *Loi sur la protection des renseignements personnels* aux sociétés d'État fédérales et à leurs filiales en propriété exclusive, suivant la recommandation du comité parlementaire d'étude. Par contre, le gouvernement n'a pas retenu celle qui voulait que le secteur privé régi par le Fédéral (banques, certaines sociétés de téléphone et de transport, par exemple) tombent sous le coup de la *Loi sur la protection des renseignements personnels*. Comme cette recommandation est l'une des rares que le Commissaire à la protection de la vie privée n'a pas endossée, nous devons nous expliquer, bien que nous ayons fourni les principaux arguments dans un rapport antérieur.

On pourrait certainement justifier l'élargissement du champ d'application de la *Loi* en dehors du gouvernement en prouvant que les atteintes à la vie privée sont endémiques.

On nous demande en effet si les banques, les compagnies de téléphone et les entreprises de télédistribution sont régies par la *Loi sur la protection des renseignements personnels*. L'inquiétude et l'appréhension du public font parfois ressortir la nécessité de protéger les renseignements personnels que constituent les transactions faites par carte de crédit.

Les risques de violation étant considérables, une telle nervosité se justifie pleinement. Ils ont beau être réels, on ne devrait imposer une réglementation contraignante aux entreprises que si elles ne font pas volontairement le nécessaire.

Les banques et les sociétés de cartes de crédit bancaires, par exemple, ont reconnu que des normes sévères de protection constituent indéniablement de bonnes pratiques commerciales. À l'instar d'autres entreprises, elles établissent leur propre code, même si ce n'est pas rapide. Les télédistributeurs, les compagnies d'assurances, les industries de publicité directe et de traitement de l'information se sont aussi dotés de codes de protection des renseignements personnels.

Dans un autre secteur, à l'instigation du Conseil de la radiodiffusion et des télécommunications canadiennes, des clauses de cette nature ont été introduites dans les nouveaux règlements des compagnies de téléphone. L'initiative du CRTC sert de modèle aux autres organismes de réglementation.

De plus en plus on encourage et on adopte une approche sectorielle, qui devient le modèle pour la prochaine génération de textes législatifs sur la protection de la vie privée. Cela va dans le sens de la décentralisation et de l'autoréglementation.

On trouve, sur le plan international, un indice de ce nouveau courant dans le projet de loi néerlandais sur la protection des données qui autorise les organismes et le secteur privé à rédiger des codes et à les soumettre à l'examen de l'autorité compétente. Celle-ci entérine le code, en apposant son sceau, si elle est d'avis qu'il est conforme à la législation. Les besoins et les dangers diffèrent, nous l'avons dit.

Une loi toujours adaptée?

Les principes généraux énoncés dans un texte de loi de grande portée risquent d'être inadaptés aux divers groupes. Il est douteux que la *Loi*, même élaborée de façon ingénieuse (ou monstrueuse),

soit un code de pratique équitable aussi valable pour les magasins de vidéo que pour l'industrie de la publicité directe, les bureaux de crédit ou la télédistribution.

Les arguments qui militent en faveur de l'extension au secteur privé des exigences de la *Loi sur la protection des renseignements personnels* vont-ils dès lors à contre-courant? Ils semblent très théoriques et ne s'appuient guère sur des preuves concrètes d'abus. En élargissant la loi inutilement, on la dévaluerait, la transformant en un fardeau au lieu d'un outil précieux.

Une telle mesure exigerait en outre un accroissement sensible du Commissariat à la protection de la vie privée. Si la *Loi* devait englober aussi les sociétés du secteur privé assujetties au pouvoir fédéral, 25 000 organismes de plus seraient visés, ce qui nécessiterait au bas mot de trois à quatre fois plus de ressources humaines et financières au Commissariat. La protection des renseignements personnels deviendrait une entreprise gigantesque, fort coûteuse, et personne n'y gagnerait.

Dans ces conditions, le Commissaire ne regrette pas que, pour l'instant, seules les sociétés d'État tombent sous le coup de la *Loi*. Mais les banques et d'autres organismes l'ont échappé belle, et cela doit leur servir d'avertissement. Les recommandations du comité parlementaire ont suffisamment de poids pour inciter le secteur privé à mettre de l'ordre chez lui s'il ne veut pas être réglementé.

Si, en matière de protection des renseignements personnels, le secteur privé préfère un régime de réglementation volontaire plutôt qu'obligatoire, il aurait tout intérêt à commencer par respecter scrupuleusement les principes établis dans les lignes directrices de l'Organisation de coopération et de développement économiques (OCDE), auxquelles le Canada adhère. Ces principes recouvrent essentiellement le même code de pratiques équitables en matière d'information que la *Loi sur la protection des renseignements personnels*. Le ministre des Affaires extérieures a prévenu les grandes sociétés canadiennes que le Canada avait ratifié ces lignes directrices et il les a invitées à s'y conformer. Mais on ne discerne pas encore de réponse à cet appel.

Autres initiatives importantes

Au risque de trop insister sur le rapport *Les prochaines étapes*, nous voudrions citer d'autres initiatives importantes.

Lorsque le gouvernement indique que « Les citoyens ne peuvent faire valoir les droits conférés par la *Loi sur la protection des renseignements personnels* s'ils n'en connaissent pas l'existence », c'est une lapalissade, mais cela doit être dit. Le programme de sensibilisation du public promis répondra à un besoin qui ne date pas d'hier.

Après cinq ans d'existence, la *Loi* est le plus souvent ignorée des Canadiens, ce qui n'a cependant pas empêché environ 170 000 personnes de demander légalement des renseignements personnels les concernant. Ces chiffres impressionnants montrent l'utilité incontestable de la *Loi*. Combien de citoyens exerceront-ils leurs droits après une campagne de publicité vigoureuse? (La protection des renseignements personnels fera-t-elle l'objet d'une publicité aussi efficace que « Participaction »?)

Expliquons maintenant une autre initiative intéressante annoncée dans *Les prochaines étapes*. On lit à l'article 37 1) de la *Loi sur la protection des renseignements personnels* que « Pour le contrôle d'application » des grands principes de la *Loi*, « le Commissaire à la protection de la vie privée peut, à son appréciation, tenir des enquêtes . . . »

Dans son énoncé de position, le gouvernement affirme que « de telles vérifications seraient souhaitables », en faisant valoir que « la *Loi* n'autorise pas expressément le Commissaire à la protection de la vie privée à tenir des enquêtes afin de vérifier la conformité à la *Loi* de façon régulière et permanente ». La *Loi* laisse ces vérifications à l'appréciation du Commissaire. Elle sera modifiée pour rendre ce pouvoir explicite.

Cette modification sera salutaire, non que le pouvoir de vérification ait été contesté ou que le Commissaire se soit senti gêné de procéder à des vérifications. (Pourquoi la *Loi* donnerait-elle un pouvoir discrétionnaire s'il ne devrait être utilisé?)

Non, l'obligation expresse de faire régulièrement enquête rappelle que les enquêteurs du Commissaire viendront. Ce message est important, parce que les contrôles systématiques contribueront à l'avenir de la protection des renseignements personnels. Il constitue une réelle garantie — au sein de l'administration et à l'extérieur.

Malheureusement, les enquêtes des vérificateurs internes dans les ministères n'ont pas augmenté comme elles l'auraient dû. Il faut encore faire accepter à la plupart des administrations que les vérifications sur la protection des renseignements devraient être aussi courantes et nécessaires que celles de la comptabilité ou de la gestion. On se demande comment, sans elles, les responsables des organismes, chargés de l'application de la *Loi sur la protection des renseignements personnels*, peuvent savoir si leur ministère la respecte.

On ne connaît qu'une poignée de ministères qui font certaines vérifications internes : Environnement Canada, la Banque du Canada et, l'année dernière, Emploi et Immigration Canada (EIC). Si un organisme aussi important et qui manipule autant de renseignements personnels que EIC a entrepris la tâche énorme d'examiner objectivement ses pratiques en la matière, quelles excuses les autres pourraient-ils invoquer pour s'y soustraire? Je regrette de constater qu'ils semblent se contenter d'attendre la venue des enquêteurs du Commissariat à la protection de la vie privée pour leur contrôle (dans certains cas, l'attente risque d'être longue). Peut-être est-ce flatteur qu'on compte sur nous, mais les vérificateurs spécialisés ne devraient pas faire le travail de base des ministères, leur rôle étant plutôt de vérifier ce qu'ont fait les vérificateurs internes.

Le rôle clé des coordonnateurs des renseignements personnels à l'égard des exigences de la *Loi sur la protection des renseignements personnels* est souligné dans *Les prochaines étapes*.

Nous nous en félicitons, parce que ce sont des professionnels de la protection de la vie privée, qui servent de véritable conscience à leur administration. Ils sont parfois tiraillés entre leur loyauté vis-à-vis de leurs collègues et de leur ministère, et le principe abstrait de la protection des données. Voilà pourquoi ce poste exige des personnalités fortes et ayant un rang hiérarchique suffisamment élevé pour qu'ils puissent s'adresser directement aux hauts fonctionnaires, comme le reconnaît lui-même maintenant le gouvernement. Cela fait deux points de marqués pour les coordonnateurs!

Les initiatives admirables et réconfortantes annoncées dans *Les prochaines étapes* ne seraient que du vent sans la volonté farouche d'y donner suite et l'octroi des ressources indispensables à leur mise en oeuvre. Il est trop tôt pour juger, mais le plan d'action prévu pour les nouvelles lignes de conduite paraît prometteur, parce que rigoureux.

Le gouvernement a tenu sa promesse de resserrer les politiques ayant trait aux NAS et au couplage des données. D'autres semblent en préparation comme, par exemple, le renforcement des dispositions applicables à la protection des renseignements personnels dans la nouvelle politique sur la sécurité; un programme de formation destiné aux fonctionnaires fédéraux, principalement aux coordonnateurs des renseignements personnels, afin qu'ils s'acquittent mieux de leurs fonctions aux termes de la *Loi sur la protection des renseignements personnels*; la mise en place par le Conseil du Trésor d'un programme de sensibilisation du public. Le personnel du Commissaire à la protection de la vie privée participe, avec des fonctionnaires du ministère de la Justice et du Conseil du Trésor, à des ateliers d'orientation organisés dans les divers sièges sociaux des sociétés d'État visées par la *Loi sur la protection des renseignements personnels*.

D'autres engagements nécessiteront plus de temps, notamment effectuer des modifications importantes de la *Loi* en vue de protéger expressément les dossiers personnels des fonctionnaires; donner au Commissariat le mandat précis d'éduquer le public; faciliter l'extension de la *Loi* à certaines sociétés d'État comme Pétro-Canada.

Quand tout cela sera enfin en place, la troisième génération de législation canadienne en matière de protection des renseignements personnels sera toujours ce qu'il y a de mieux sur le plan international, et ce n'est pas là de l'orgueil mal placé.

Les grands absents

Mais d'autres réaménagements laissés de côté auraient pu améliorer le tableau. Nous déplorons particulièrement l'absence, dans la *Loi*, d'un mécanisme permettant à une personne d'empêcher la divulgation de renseignements personnels en attendant le règlement d'un différend sur l'opportunité de cette divulgation. Nous nous sommes expliqués sur cette question dans le rapport de l'année dernière :

« Il est anormal que les personnes à qui on refuse l'accès à leurs renseignements personnels puissent demander aux tribunaux l'examen de la décision, mais qu'ils ne puissent pas en appeler de la décision d'un ministère de communiquer leurs renseignements personnels à des tiers. »

Il ne s'agit plus maintenant d'anomalie, mais d'incongruité : la *Loi sur l'accès à l'information* prévoit un mécanisme qui informe les sociétés dont les renseignements de nature commerciale sensibles peuvent être divulgués et qui leur permet de s'exprimer. Par contre, la *Loi sur la protection des renseignements personnels* n'accorde pas les mêmes droits aux personnes dont des renseignements personnels sensibles peuvent être divulgués. Il faut pouvoir protéger de la même façon les renseignements personnels et les renseignements de nature commerciale. En modifiant la *Loi*, le gouvernement mettrait fin à cette distorsion.

Revenons-en à la vieille controverse de l'article 19 de la *Loi*. Cet article est moins irritant qu'il y a quatre ans, au moment de l'entrée en vigueur de la *Loi*, mais il est toujours malcommode et peu satisfaisant. Il oblige les institutions du gouvernement fédéral à refuser de communiquer des renseignements personnels qui ont été obtenus à titre confidentiel d'une province. En 1983, nerveuses et sur la défensive, la plupart des provinces ont réclamé le secret des renseignements déjà fournis aux ministères fédéraux et de tous ceux qui pourront leur être fournis ultérieurement.

Toujours contraires à la *Loi sur la protection des renseignements personnels*, ces revendications générales sont particulièrement gênantes dans certains cas. Au Service correctionnel du Canada (SCC) et à la Commission nationale des libérations conditionnelles (CNLC), les requérants se voient refuser systématiquement l'accès aux renseignements de leur dossier pour la seule raison qu'ils ont été communiqués par une police provinciale ou municipale ou par une commission de libération ou un service correctionnel provincial. Le SCC et la CNLC ne peuvent divulguer le moindre renseignement, même le plus neutre, alors qu'ils le feraient facilement s'il était d'origine fédérale.

Au lieu de rejeter purement et simplement les nombreuses plaintes parce que les ministères fédéraux sont tenus de cacher l'information, le Commissaire à la protection de la vie privée a encouragé le SCC et la CNLC à conclure avec les provinces des ententes qui permettraient de traiter les renseignements conformément à la *Loi sur la protection des renseignements personnels*, comme s'ils étaient d'origine fédérale.

Et ça marche! (ou presque)

Ce procédé a donné quelques résultats encourageants : des accords ont été conclus avec le Québec, le Nouveau-Brunswick, la Nouvelle-Écosse, l'Île-du-Prince-Édouard et le Yukon. Mais d'autres provinces ont refusé, notamment l'Ontario, ce qui est d'autant plus déconcertant qu'il a adopté, le 1er janvier 1988, sa propre loi d'accès aux renseignements personnels, qui permet de divulguer des renseignements confidentiels fédéraux comme si c'étaient les siens — deux poids, deux mesures . . .

Malheureusement, il semble que le Commissaire ne pourra raisonnablement pas régler les plaintes portant sur des renseignements provenant de l'Ontario, du Manitoba, de la Saskatchewan, de l'Alberta ou de la Colombie-Britannique. Les cas ont pris trop de retard, il n'y a plus d'espoir. Il ne reste plus qu'à autoriser le recours à l'article 19. Nous regrettons que des critères géographiques déterminent les droits à la protection des renseignements personnels. L'accès ou le non-accès aux renseignements dépendront de leur provenance, suivant les provinces. C'est tout simplement inacceptable.

Reste un dernier espoir — le règlement politique. Si le ministre de la Justice et le Solliciteur général du Canada pouvaient conclure des ententes avec les provinces, cette discrimination arbitraire pourrait disparaître. La cause mérite un regain d'effort.

Tandis qu'on « polit » les règlements canadiens de troisième génération en matière de protection des données, de nouvelles questions urgentes apparaissent.

Vers une politique sur le SIDA

La plus délicate, et la plus lourde de conséquence, tient à la réaction fédérale au syndrome d'immuno-déficience acquise (le SIDA). Dans quelles situations, s'il en existe, faut-il autoriser les tests obligatoires de dépistage du SIDA? Comment le gouvernement doit-il employer les renseignements personnels relatifs au SIDA qu'il détient? À qui et dans quelles circonstances peut-on divulguer des renseignements personnels sur le SIDA? L'opprobre du SIDA oblige-t-il les pouvoirs publics à le traiter différemment des autres maladies transmissibles? Quelle cote de sécurité les renseignements sur le SIDA doivent-ils recevoir? Voilà des questions fondamentales pour l'élaboration d'une politique fédérale de protection des renseignements personnels sur le SIDA.

Une telle politique est l'affaire du gouvernement et des législateurs, pas du Commissaire à la protection de la vie privée. Il insistera certes vigoureusement sur les intérêts de la protection des renseignements personnels, mais les responsables devront tenir compte de nombreuses questions contradictoires.

Partant du principe que le manque d'information ne doit pas empêcher une politique de protection de la vie privée cohérente et humaine, le Commissariat a entamé une étude du SIDA dans son optique, afin de fournir des conseils bien informés. Les ministères concernés ont collaboré étroitement à ces travaux.

Pour l'administration fédérale, la question du SIDA se présente sur plusieurs fronts — dans ses rapports avec les détenus, les immigrants, ses employés (agents du service extérieur, membres des Forces armées, gardiens de prison ou infirmières). Santé et Bien-être Canada encourage les employeurs à formuler des lignes de conduite sur le SIDA, mais le premier employeur du pays, le gouvernement fédéral, n'en possède toujours pas.

L'absence de politique générale ne signifie pas pour autant absence de tests de dépistage. Par exemple, la Défense nationale a lancé un programme de cette nature, à cause du ministère américain de la Défense, qui oblige tous les étrangers inscrits à ses cours de formation à prouver qu'ils ne sont pas séropositifs. Plus de 1 000 employés du ministère canadien de la Défense nationale, civils et militaires, suivent ces cours tous les ans.

Il convient de se demander sérieusement si la politique américaine en matière de SIDA devrait dicter la conduite du Canada. Mais cela n'irait pas sans conséquences. Au cas où, par exemple, le Canada rejetterait le dépistage obligatoire, qu'adviendrait-il de la carrière des employés exclus des cours américains de la Défense parce qu'ils ont refusé de se soumettre au test ou que le test est positif?

Si le Canada est partisan de tests purement volontaires, il lui faut une politique bien définie, qui précise la destination des renseignements et les circonstances dans lesquelles ils pourront être communiqués à des tiers.

Dossiers du SCRS

Une autre question non réglée, qui a été très débattue pendant l'année, est de trouver l'équilibre entre l'accessibilité et le secret dans le domaine de la sécurité et du renseignement. Le Service canadien du renseignement de sécurité (SCRS) est assujetti à la *Loi sur la protection des renseignements personnels*. Malgré cela, très peu de requérants ont eu accès à leur dossier ou ont même reçu confirmation de l'existence d'un dossier les concernant. Cela n'est guère étonnant, le SCRS travaille en silence. On ne peut lui reprocher de ne pas avoir respecté la *Loi* et, compte tenu des conditions particulières de son travail, le Parlement a prévu des dispenses précises sur les exigences de divulgation.

Mais arrive un moment où, soit que l'information perde de son caractère confidentiel avec le temps, soit qu'elle paraisse bien banale, il devient difficile d'expliquer en quoi la divulgation nuit au Service du renseignement.

La question fait l'objet d'une étude en collaboration avec le SCRS, en vue de déboucher sur la formulation d'une politique claire et acceptable.

Bienvenue au club

La grande nouvelle en matière de protection des renseignements personnels au Canada cette année n'est pas du domaine fédéral.

L'entrée en vigueur de la *Loi ontarienne sur l'accès à l'information et la protection de la vie privée* constitue en effet un grand tournant dans la protection des données au pays. Comme elle s'applique aux organismes de la province, la nouvelle loi de l'Ontario permet de protéger les intérêts de millions de citoyens.

Le commissaire de l'Ontario, M. Sidney Linden, et le Commissariat fédéral travaillent en étroite collaboration, dans une atmosphère cordiale. Ils ont échangé des visites et tenu des consultations utiles.

L'adoption des lois provinciales fortes en matière de protection des données (la loi générale du Québec a pris effet en 1984) ne peut que renforcer les lois fédérales et provinciales. Ni le droit à la protection de la vie privée ni la liberté ne doivent être divisibles.

LES PROBLÈMES — anciens et nouveaux

LE COUPLAGE DES DONNÉES ET LE NAS

Au début de ce rapport, nous avons mentionné, parmi les bonnes nouvelles, que le gouvernement avait pris l'engagement important d'instituer des mesures de contrôle sur le couplage des données et l'emploi du numéro d'assurance sociale.

Le pouvoir de la technologie de l'information, sa souplesse et son omniprésence peuvent être les plus grands obstacles à l'efficacité de la *Loi sur la protection des renseignements personnels* dans les dix prochaines années.

L'un des objectifs capitaux de la *Loi* était d'empêcher que l'État ne constitue un fichier centralisé de renseignements complets sur un individu en particulier, ce qui est maintenant devenu techniquement faisable étant donné que le gouvernement détient plus de renseignements informatisés. En utilisant les numéros d'assurance sociale (NAS), qui servent de numéros d'identification personnels de l'Administration, les techniciens d'interconnexion des ordinateurs réussiraient à faire ce qui paraissait autrefois — peut-être par excès de confiance — très improbable.

L'annonce du gouvernement est donc opportune. Le Commissariat à la protection de la vie privée a étroitement collaboré avec les fonctionnaires du Conseil du Trésor chargés d'élaborer une politique détaillée de contrôle. Le Canada pourrait bien disposer des mesures de contrôle les plus strictes du monde concernant l'emploi de l'informatique pour comparer et compiler les renseignements extraits de fichiers conservés dans des bases de données indépendantes.

La politique concernant le couplage des données

Voici les grandes lignes de la nouvelle politique en matière de couplage des données :

* il est interdit de coupler des données sans l'autorisation écrite du responsable de l'institution gouvernementale concernée, généralement le ministre;

* les projets de couplage de données doivent être justifiés, notamment par :

  — une étude préliminaire sur la conformité d'un couplage des données avec la *Loi sur la protection des renseignements personnels*; et

  — une étude des coûts et des avantages du projet de couplage par rapport au risque de violation de la vie privée des individus;

* les couplages de données seront consignés au Répertoire de renseignements personnels;

* les projets de couplage des données doivent être portés à l'attention du Commissaire à la protection de la vie privée, en lui remettant une copie du rapport préliminaire 60 jours avant le début de l'opération;

* les renseignements extraits par couplage des données doivent être assujettis à une vérification indépendante avant de servir à des décisions touchant directement un individu; et

* un individu doit pouvoir réfuter les renseignements issus d'un couplage des données avant l'application de toute mesure le concernant.

La politique concernant le numéro d'assurance sociale

L'engagement de redonner au numéro d'assurance sociale (NAS) son rôle initial de numéro d'identification spécialisé pour certains programmes sociaux est essentiel au contrôle du couplage des données. Dorénavant, seuls les programmes dûment autorisés par le Parlement emploieront ce numéro. Les autres le remplaceront progressivement par des numéros d'identification uniques, ce qui réduira la possibilité de coupler les données extraites de bases de données indépendantes en rendant l'opération beaucoup moins rentable.

La nouvelle politique consistera à :

* faire cesser, sauf autorisation du Parlement, la collecte et l'utilisation du numéro d'assurance sociale par le gouvernement;

* examiner toutes les collectes et les utilisations actuelles du numéro d'assurance sociale en fonction des exigences de la *Loi sur la protection des renseignements personnels*;

* exiger que les collectes et les utilisations actuelles du NAS non prescrites par la loi cessent, sauf si le Conseil du Trésor est d'avis que les avantages du maintien l'emportent sur les risques en matière de protection des renseignements personnels;

* empêcher que l'on refuse à quiconque un droit, un avantage ou un privilège, ou que l'on impose une sanction parce qu'un individu refuse de fournir son numéro d'assurance sociale, à moins que la communication du numéro soit exigée par la loi;

* préciser aux individus auxquels on demande de fournir leur numéro d'assurance sociale quel usage en sera fait, si la communication est impérative ou volontaire, et si un refus peut avoir des conséquences.

Nous applaudissons certes à ces initiatives, mais nous ne pouvons nous empêcher de craindre que le Parlement ne contourne ces lignes directrices et la *Loi sur la protection des renseignements personnels* en autorisant de nouveaux programmes d'interconnexion des ordinateurs ainsi que de nouvelles utilisations du NAS. Le Congrès américain a, par exemple, autorisé l'interconnexion à grande échelle, principalement pour prévenir et détecter les fraudes contre les programmes de l'État.

Il est difficile d'opposer des arguments convaincants à cette démarche, qui peut constituer, au Canada aussi, une justification importante pour la prolifération de l'interconnexion. On constate néanmoins de plus en plus aux États-Unis que cette pratique fait réaliser moins d'économies que cela n'avait été prétendu. Le soin apporté à la conception d'un programme et le recours à d'autres techniques d'application s'avèrent aussi rentables que le couplage des données, tout en offrant l'avantage de préserver la vie privée de sujets innocents.

Comme nous l'avons dit, certaines « bonnes raisons » d'ordre social peuvent l'emporter sur la protection des renseignements personnels. Mais c'est au Parlement de faire ces jugements, de la façon la plus éclairée possible. Un élément clé de tout nouveau projet de couplage des données est l'étude rigoureuse de rentabilité. Même à des fins sociales fort louables, le Parlement ne devrait pas donner son feu vert sans soupeser les coûts et les avantages d'un côté, et le risque d'intrusion dans la vie privée, de l'autre.

« USAGES COMPATIBLES »

Maintenant que la *Loi sur la protection des renseignements personnels* et la nouvelle politique restreignent le couplage des données, les administrations fédérales pourraient être tentées d'interpréter les « usages compatibles » de façon suffisamment large pour interconnecter des fichiers indépendants.

La *Loi* ne prévoit pas de mécanisme qui autoriserait le Commissaire à la protection de la vie privée (ou quelqu'un d'autre) à contester en cour la communication abusive de renseignements. Les ministères pourraient miser sur la clause des « usages compatibles » pour contourner un contrôle effectif du couplage des données.

La *Loi* ontarienne *sur l'accès à l'information et la protection de la vie privée* s'efforce d'empêcher une interprétation trop large en proposant une définition de « fin compatible ». L'article 43 prévoit que :
« Seule constitue une fin compatible . . . , la fin invoquée à l'appui de l'utilisation ou de la divulgation de renseignements personnels à laquelle le particulier concerné par les renseignements pourrait raisonnablement s'attendre lorsque ceux-ci ont été obtenus du particulier directement. »

Le Commissaire à la protection de la vie privée recommande donc deux modifications à la *Loi sur la protection des renseignements personnels* : une définition destinée à clarifier l'interprétation des « usages compatibles »; et le droit pour le Commissaire à la protection de la vie privée ou tout individu lésé de chercher un recours judiciaire contre la décision d'une institution du gouvernement d'utiliser ou de communiquer des renseignements personnels.

Les difficultés auxquelles il faut s'attendre si on veut subordonner la technologie aux principes de la protection des renseignements personnels ne doivent pas nous faire oublier l'importance des mesures de contrôle citées.

PROTECTION DE LA VIE PRIVÉE DES DÉTENUS EN LIBÉRATION CONDITIONNELLE ET INTERNÉS

Comme il l'avait promis dans son dernier rapport, le Commissaire à la protection de la vie privée a examiné les lignes de conduite de la Commission nationale des libérations conditionnelles (CNLC) et du Service correctionnel du Canada (SCC) sur l'utilisation et la communication des renseignements. Il a aussi reçu pour analyse un projet de code révisé de la CNLC sur ce sujet, et il s'est penché sur les orientations du SCC dans le cadre d'une vérification décrite ailleurs dans ce rapport.

À la suite de son examen, le Commissaire a désigné trois règles qui lui ont paru contraires à la *Loi sur la protection des renseignements personnels*. Il s'agissait des communications à la GRC, aux victimes, aux médias et au public.

Communication à la GRC

Dans leurs lignes de conduite, la CNLC et le SCC autorisent la divulgation de renseignements personnels sur les détenus internés et en libération conditionnelle à la GRC parce qu'ils considèrent ces communications comme des « usages compatibles » de l'information (alinéa 8(2)*a*) de la *Loi*). C'est oublier que la GRC peut chercher des renseignements sur un autre acte criminel que celui qui a entraîné la condamnation.

Le SCC et la CNLC ne respectent pas les exigences de la *Loi sur la protection des renseignements personnels* voulant que les communications à la GRC doivent être faites seulement à la suite d'une demande écrite qui justifie la requête et qui indique le renseignement recherché. À la demande du Commissaire à la protection de la vie privée, il faut lui envoyer copie des requêtes et un relevé des renseignements transmis.

Comme les deux organismes considèrent que les communications à la GRC constituent des « usages compatibles », ils n'exigent pas de demande écrite et n'envoient pas de relevé pour l'examen du Commissaire.

Même si les demandes de la GRC sont « compatibles », la *Loi sur la protection des renseignements personnels* oblige le SCC et la CNLC à consigner les utilisations dans le Répertoire de renseignements personnels et, en l'absence de liste, à avertir le Commissaire de la communication et de son usage.

Or le Commissaire n'a jamais reçu d'avis concernant les communications à la GRC, même si ces divulgations sont pratique courante. En outre, beaucoup des relevés pertinents des répertoires du SCC et de la CNLC n'indiquent pas que des renseignements peuvent être fournis à la GRC.

Cette pratique entrave manifestement l'examen indépendant du Commissaire prescrit par la *Loi* au sujet des communications.

Communication aux victimes

En règle générale, le SCC et la CNLC préviennent les victimes d'un acte criminel de la date de libération d'un détenu, des conditions de sa libération et de sa destination, en considérant qu'il s'agit d'usages conformes en vertu de l'alinéa 8(2)*a*).

Le Commissaire à la protection de la vie privée n'est pas d'accord. Pour que ce soit un usage compatible, il faudrait avoir des raisons de croire que la personne harcèlerait la victime, lui ferait du mal ou la mettrait en danger de toute autre façon, ou que des raisons d'intérêt public justifient nettement la communication (sous-alinéa 8(2)*m*)(i) de la *Loi*). Le Commissaire a incité les deux organismes à évaluer chaque cas individuellement, au lieu d'accorder une autorisation générale pour ce genre de communication.

La divulgation de renseignements personnels à des tiers violait les droits à la vie privée des détenus, risquant de compromettre la réintégration de l'individu dans la société, et même de lui faire courir des risques.

Le SCC et la CNLC ont accepté de préparer une nouvelle politique sur les communications aux victimes qui exercera un contrôle plus rigoureux.

Communication aux médias et au public

Dans leurs lignes de conduite, le SCC et la CNLC ont autorisé la divulgation des casiers judiciaires aux médias et au public. Ils considéraient en effet que le casier judiciaire d'un individu n'est pas protégé par la *Loi sur la protection des renseignements personnels*, parce que c'est une information à laquelle le public a accès dans les archives du tribunal.

Le Commissaire a rejeté cette interprétation, car sinon, on pourrait constituer le casier judiciaire de n'importe quel citoyen et le divulguer au grand public — ce qui est une interprétation large inacceptable de l'expression « renseignements personnels auxquels le public a accès ».

S'il est vrai qu'on peut trouver la condamnation d'un individu dans les dossiers du tribunal, auquel le public a accès, peut-être éparpillés dans tout le pays (et à l'étranger), cela ne signifie pas pour autant que les listes cumulatives de condamnations préparées par les organismes d'application de la loi ou des établissements de correction sont, elles aussi, accessibles au public. L'effet produit par des dossiers cumulatifs est beaucoup plus fort que celui d'une condamnation isolée. La différence réside notamment dans la somme de renseignements et les conséquences possibles de leur communication. D'autant qu'avec les dossiers cumulatifs, il y a plus de risques d'inexactitudes et d'insuffisances.

Ajoutons que le Solliciteur général applique un principe strict de secret pour la GRC en sa qualité d'organisme national de garde des renseignements versés aux casiers judiciaires. En vertu de ce principe, il est interdit de communiquer des renseignements au public ou aux médias.

Le SCC et la CNLC ont modifié ultérieurement leur politique en supprimant l'autorisation de communiquer au public le casier judiciaire d'un contrevenant.

LA PROTECTION DE LA VIE PRIVÉE AU TRAVAIL

La protection des renseignements personnels dans le milieu professionnel tiendra une place croissante au Commissariat quand les sociétés d'État et leurs filiales seront assujetties à la *Loi sur la protection des renseignements personnels*. Les effectifs combinés des 130 organismes supplémentaires l'emportent sur ceux des 147 administrations déjà couvertes par la Loi. Pour compliquer la situation, certaines grandes sociétés d'État (comme Air Canada et Petro Canada) rivalisent avec le secteur privé, peu soucieux quant à lui de protéger les renseignements personnels, et où la sélection et la surveillance des employés sont plus répandues.

Pendant l'exercice, les fonctionnaires se sont inquiétés du nombre de renseignements les concernant susceptibles d'être communiqués au nom de la *Loi sur l'accès à l'information*. Ils n'ont pas trouvé normal, par exemple, que la direction demande trop de détails sur leur état de santé ou que des fonctionnaires de longue date fassent l'objet de nouvelles enquêtes sévères de sécurité et de fiabilité. Ils se sont dits préoccupés des risques d'atteinte à leur vie privée et à leur dignité au travail par suite du dépistage des drogues et du SIDA ou de la surveillance électronique.

Possibilités d'accès aux données touchant les fonctionnaires

Le rapport annuel 1986–1987 du Commissaire résumait une enquête sur le respect du *Code relatif aux conflits d'intérêt* du gouvernement par rapport aux exigences de la *Loi sur la protection des renseignements personnels*. Le Commissaire a conclu que la *Loi* ne pouvait empêcher la communication de renseignements personnels sur des fonctionnaires quand des tiers le demandent en invoquant la *Loi sur l'accès à l'information*.

Il y a eu justement cette année plusieurs cas de communications faites dans ces conditions et qui ont déclenché une série de plaintes.

Le ministère de la Défense nationale (MDN) et la Gendarmerie royale du Canada (GRC) ont, par exemple, tous deux divulgué la liste de tous les employés, militaires et civils, de la Région de la capitale nationale qui gagnaient 42 000 $ par an et plus, avec leur rang, leur classification et leur secteur d'emploi.

Dans ces cas, décrits en détail dans la section des plaintes de ce rapport, le Commissaire à la protection de la vie privée a conclu qu'il ne s'agissait pas de renseignements « personnels » d'après le paragraphe 3(j) de la *Loi sur la protection des renseignements personnels* et qu'ils ne pouvaient donc être protégés. Les ministères sont même tenus de divulguer cette information. Mais il n'y a pas de raison que des particuliers soient la cible des commerçants pour la simple raison qu'ils sont fonctionnaires. Comme pour l'enquête sur les conflits d'intérêt, ces divulgations n'ont réussi qu'à souligner la nécessité de mieux protéger les renseignements que l'Administration détient sur ses employés. C'est crucial pour les fonctionnaires qui occupent des postes délicats, à haute sécurité, car leur sécurité pourrait être menacée si leur identité était rendue publique.

Le gouvernement a abordé ces questions dans *Les prochaines étapes*, et a promis de modifier la définition des renseignements personnels : « On précisera que les renseignements délicats touchant les employés, comme les déclarations relatives à l'équité en matière d'emploi ou aux conflits d'intérêts et les évaluations de rendement, doivent être traités comme des renseignements personnels et protégés par la *Loi sur la protection des renseignements personnels* ».

Mais cela ne résoudra pas le dilemme des ministères aux prises avec des demandes de listes d'employés à des fins commerciales ou de sollicitation.

Communication de renseignements médicaux

Un fonctionnaire s'est plaint qu'on lui ait refusé des prestations de congé de maladie parce qu'il n'avait pas voulu donner à son supérieur les détails de sa maladie ou de son invalidité. Le ministère a fait valoir qu'il lui fallait ces renseignements en raison du nombre de congés de maladies déjà pris par l'intéressé; parce qu'il se souciait de l'état de santé de son employé et des conséquences possibles pour sa sécurité et celle de ses collègues au travail. Il a également souligné les éventuelles répercussions d'une invalidité à long terme.

Le Commissaire à la protection de la vie privée n'a pas contesté la nécessité pour un employeur d'avoir la preuve que son employé ne peut remplir ses fonctions à cause d'une maladie ou d'une blessure. Mais l'article 4 de la *Loi sur la protection des renseignements personnels* interdit la collecte de détails précis sur une maladie, une blessure ou d'autres conditions médicales. Les employeurs qui s'interrogent sur le bien-fondé de certaines demandes de congé peuvent vérifier l'état de santé et l'aptitude au travail de leur subordonné en l'adressant à un médecin du ministère de la Santé et du Bien-être.

Le ministère a accepté cette formule et le Commissaire a recommandé que toutes les administrations adoptent une ligne de conduite semblable.

Enquêtes de fiabilité et de sécurité

Le Commissaire à la protection de la vie privée a indiqué l'an dernier que si la nouvelle politique du gouvernement en matière de sécurité n'enfreignait pas la *Loi sur la protection des renseignements personnels*, elle donnait peu de latitude aux ministères. C'est ainsi qu'on a vu des préposés à l'enlèvement de la neige des patinoires du canal Rideau, à Ottawa, obligés d'aller fournir leurs empreintes digitales. Après des pourparlers avec le Conseil du Trésor, la politique a été modifiée et permet désormais aux ministères de juger si la vérification du crédit et des empreintes digitales doit nécessairement faire partie du contrôle renforcé de fiabilité.

N'empêche que la protection des renseignements concernant les fonctionnaires recueillis à cause de cette politique devrait entrer dans la nouvelle définition des renseignements personnels (voir plainte type page 36) à changer dans la *Loi*. Le Commissaire craint par ailleurs que trop de postes de la fonction publique exigent l'autorisation sécuritaire. Étant donné que les enquêtes indispensables pour bénéficier des cotes confidentiel, secret ou ultra-secret entraînent des recherches approfondies des antécédents, seuls les particuliers dont les fonctions exigent une telle enquête devraient y être assujettis. Le Commissaire se penchera sur ce dossier pour empêcher tout arbitraire en ce domaine.

Dépistage du SIDA

On ne peut faire abstraction du syndrome d'immuno-déficience acquise, le SIDA, maladie actuellement incurable et mortelle, qui frappe toutes les couches de la société et pose des problèmes complexes et graves.

Les principes et les initiatives que les pouvoirs publics adoptent pour lutter contre l'épidémie de SIDA doivent concilier deux objectifs importants, mais parfois antagoniques : la protection des droits individuels et celle de la santé publique.

La collecte, l'utilisation et la communication par le gouvernement des renseignements liés au SIDA doivent évidemment respecter la *Loi sur la protection des renseignements personnels*. Mais faut-il les traiter différemment d'autres renseignements personnels sur les maladies transmissibles? La *Loi* interdit-elle ou limite-t-elle le dépistage du SIDA? À quoi peuvent servir les renseignements sur le SIDA? à qui peut-on les communiquer? dans quel but?

Comme le texte de la *Loi* n'est pas clair et qu'un certain nombre de questions difficiles doivent être examinées, le Commissaire à la protection de la vie privée a entamé une étude en étroite collaboration avec les principaux ministères fédéraux. Il prépare un document de travail qui devrait permettre d'élaborer une politique sur les renseignements relatifs au SIDA en ménageant à la fois les droits à la vie privée et la protection de la santé publique.

La sélection des fonctionnaires

La *Loi sur la protection des renseignements personnels* ne prévoit pas expressément la sélection et les techniques de surveillance comme les tests de dépistage des drogues, le recours au polygraphe ou la surveillance électronique. Le Comité parlementaire a recommandé l'élargissement de la *Loi* en faisant entrer le respect de l'intimité physique dans la protection des renseignements personnels et en donnant au Commissaire à la protection de la vie privée le mandat d'observer les nouvelles techniques de surveillance. Le gouvernement a rejeté cette recommandation, parce qu'il était d'avis que la *Loi* devait continuer à protéger les données et à ne s'appliquer qu'à la collecte, à l'utilisation et à la communication des renseignements personnels provenant de la surveillance et des tests.

La *Loi* régit bien l'usage et la communication des résultats. Mais l'observation de l'article 4 à l'effet que « les seuls renseignements personnels que peut recueillir une institution fédérale sont ceux qui ont un lien direct avec ses programmes et ses activités » continue à créer des difficultés. La plus importante pourrait d'ailleurs bien tenir à la fiabilité des méthodes de sélection, parce que l'emploi de tests non fiables pourrait lui-même enfreindre l'article 4. Pareillement, les techniques indiscrètes de sélection, de dépistage et de surveillance peuvent constituer des exercices interdits de collecte des données si d'autres moyens, moins indiscrets, existent.

Le Commissaire à la protection de la vie privée continuera à observer attentivement la surveillance et le recours aux tests de dépistage effectués par le gouvernement à l'égard des candidats et des fonctionnaires, et il encouragera l'élaboration de lignes directrices devant protéger les intérêts des particuliers en matière de protection des renseignements personnels.

Fichiers de renseignements inconsultables

Au terme des vérifications d'application menées sur les cinq derniers fichiers de renseignements inconsultables, un seul a été jugé bien constitué, celui de la Défense nationale MDN/P-PU-040 (Dossiers sur l'information de sécurité et de renseignement). (Pour qu'un fichier soit bien constitué, il faut que chacun des dossiers qui le forment soit examiné pour s'assurer qu'y « dominent » des renseignements personnels obtenus par un organisme d'enquête, ou dont la divulgation pourrait porter préjudice à la conduite des affaires internationales, à la défense, à l'exécution de la loi au Canada.)

En dehors du fichier de la Gendarmerie royale du Canada GRC/P-PU-015 (Documents sur le renseignement criminel opérationnel), les autres fichiers déclarés inconsultables dans le rapport de l'année dernière sont maintenant traités comme ouverts, et leur statut d'exception sera annulé.

Le Commissaire à la protection de la vie privée a jugé que le dernier fichier inconsultable, celui de la GRC, avait été, lui aussi, constitué incorrectement. Il a donc recommandé au Solliciteur général d'annuler le décret actuel de classement comme fichier inconsultable, et de faire prendre un nouveau décret valide s'il estimait nécessaire de maintenir le statut d'exception. Le Solliciteur général n'était pas d'accord parce que, selon lui, les dossiers qui, aux dires du Commissaire, n'avaient pas été examinés à l'origine ne faisaient en réalité pas partie du fichier inconsultable.

Les discussions entamées pour régler ce litige factuel progressent. En attendant, le Solliciteur général maintiendra le statut d'exception du fichier GRC/P-PU-015.

Direction des plaintes

Le Commissariat a reçu 696 plaintes au cours de l'année et a terminé 661 enquêtes, dont 155 (23 pour cent) ont été déclarées justifiées par le Commissaire, et 492 (74 pour cent) non fondées. Les 14 dernières (3 pour cent) ont été abandonnées ou retirées.

Deux nouveautés sautent aux yeux cette année par rapport à 1986–1987. On constate tout d'abord un recul net des plaintes liées aux retards, qui représentent 22 pour cent de l'ensemble, contre 56 pour cent l'an dernier. Cette évolution assez surprenante explique en grande partie qu'il y ait moins de plaintes fondées cette année, puisqu'en général ce genre de plaintes est justifié.

Deuxième changement, nous avons reçu 66 plaintes de moins (8,6 pour cent). Pour la première fois en cinq ans, les plaintes n'ont pas augmenté d'au moins 10 pour cent. Si cette diminution est un élément positif — après tout, l'objectif est que les ministères donnent satisfaction à tous les usagers de la *Loi* — on ne peut dire pour autant qu'il n'y a pas d'ombre au tableau.

Il est certain que les ministères respectent maintenant mieux les délais de réponse, mais nous recevons un plus grand nombre de plaintes touchant des questions de fond.

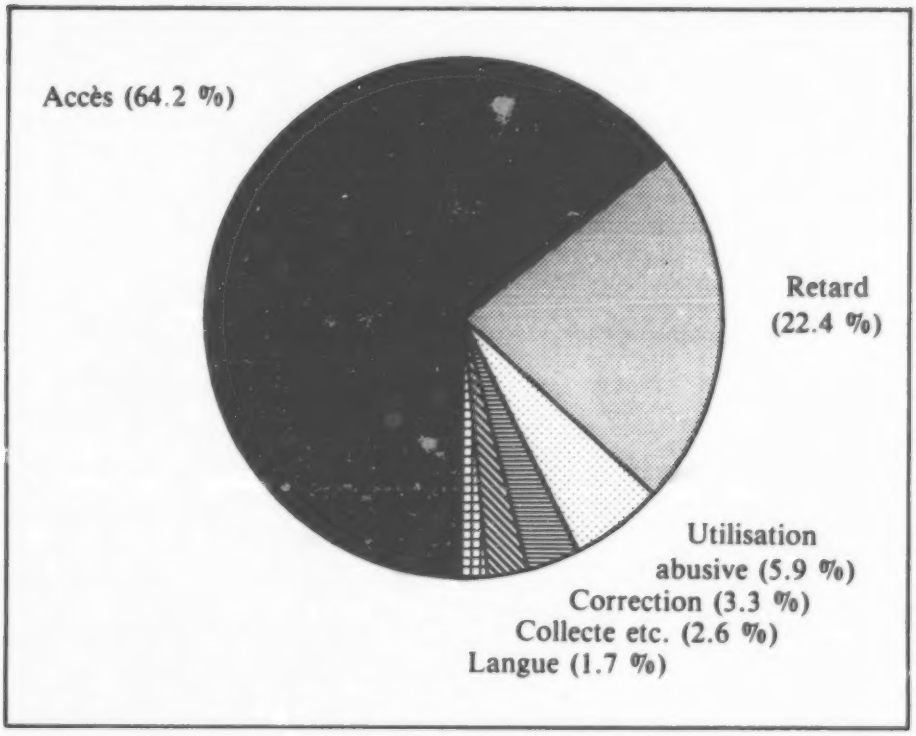
Près de 64 pour cent des plaintes réglées cette année, contre seulement 36 pour cent l'an passé, portaient sur le refus d'accès aux renseignements personnels. Et nous nous inquiétons de la multiplication des cas où, au lieu de tarder à répondre, les ministères ont refusé de fournir les renseignements. Il serait prématuré de parler de tendance après un an, mais nous suivrons de près l'augmentation des refus d'accès.

Les sept enquêteurs ont chacun étudié en moyenne 99 dossiers pour l'année, ce qui paraît plus raisonnable que les 109 de l'an dernier, mais les plaintes étant plus complexes, il leur a fallu en réalité travailler davantage. Et en plus des enquêtes menées sur les plaintes, ils ont répondu à 1 248 demandes de renseignements, presque 10 pour cent de plus que l'an passé (voir page 50).

Au total, cela représente une charge de travail intenable qui pourrait entraîner un retard inacceptable dans les dossiers. Pour cette raison, et étant donné le surcroît de travail auquel il faut s'attendre quand les sociétés d'État seront assujetties à la *Loi*, nous sommes heureux d'annoncer que nous avons été autorisés à recruter neuf employés supplémentaires, dont des enquêteurs.

Les affaires qui suivent montrent le genre de plaintes dont le Commissariat s'est occupé pendant l'exercice. Nous avons supprimé tous les détails qui auraient permis une identification parce que la *Loi* exige que les enquêtes soient secrètes.

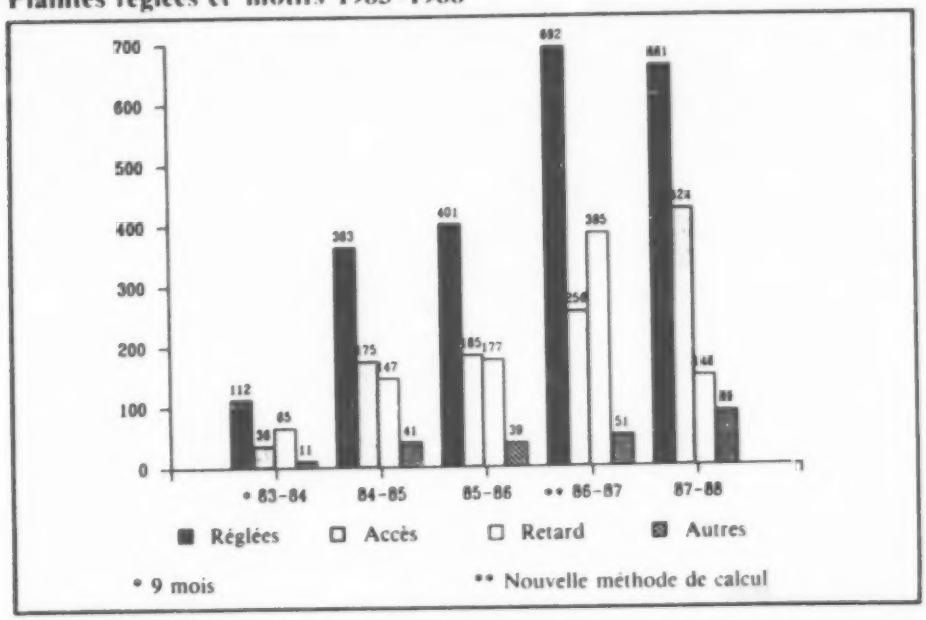
Plaintes réglées par motifs 1987-1988



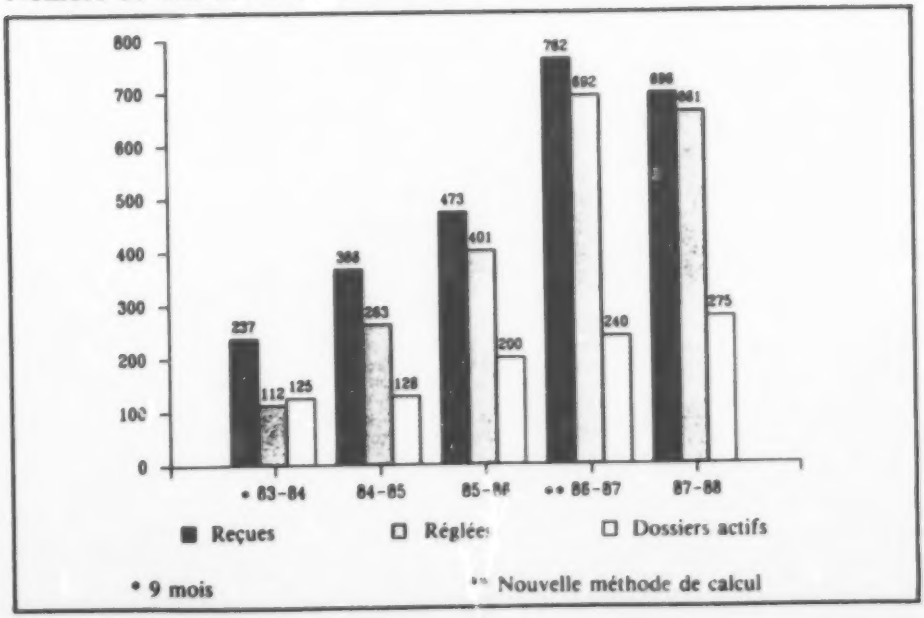
Plaintes par motifs et résultats

Motifs	Abandonnée	Justifiée	Rejetée	Total
Utilisation abusive	2	6	31	39
Accès	10	54	360	424
Correction	—	2	20	22
Langue	—	1	10	11
Répertoire	—	—	—	—
Collecte/ conservation/ retrait	1	1	15	17
Retard	1	91	56	148
Total	**14**	**155**	**492**	**661**

Plaintes réglées et motifs 1983-1988



Nombre de dossiers 1983-1988



RECOURS À LA *LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS*

Selon les derniers chiffres du Conseil du Trésor (31 décembre 1987), les demandes adressées aux ministères en vertu de la *Loi sur la protection des renseignements personnels* continuent à croître. On en a enregistré 12 013 pendant le seul trimestre allant du 1er octobre au 31 décembre 1987, ce qui bat tous les records. En tout, depuis l'entrée en vigueur de la *Loi*, le 1er juillet 1983, un total de 159 835 demandes ont été déposées.

Délais de réponse

Malgré l'accroissement des demandes, les ministères semblent suivre assez bien le mouvement.

De 1983 à 1986, 53 pour cent seulement des requérants ont reçu une réponse dans les 30 jours prévus par la *Loi*; 16 pour cent ont dû attendre de 31 à 60 jours, et 31 pour cent ont attendu encore plus longtemps — ce qui constituait, techniquement, un refus d'accès. Par comparaison, cette année, 65 pour cent des demandes ont été réglées en 30 jours; 22 pour cent en 60 jours, et 13 pour cent en plus de 60 jours. Cette nette amélioration (due à l'expérience acquise par les ministères, à l'augmentation de leurs ressources et à leur somme de travail) explique le recul des plaintes liées aux retards.

Communications complètes

Un peu plus de 64 pour cent des requérants reçoivent tous les renseignements qu'ils ont demandés (parfois plus). Près de 22 pour cent s'en font refuser une partie, en général parce que les renseignements concernent une tierce personne (47 pour cent des cas), qu'ils proviennent d'une province qui les considère confidentiels (21 pour cent) ou qu'ils ont trait à l'exécution de la loi et aux enquêtes, ce qui inclut les renseignements de la GRC en sa qualité de police provinciale (17 pour cent).

Six pour cent des requérants ne reçoivent rien : un pour cent, parce qu'il s'agit de renseignements auxquels le public a déjà accès ou de documents confidentiels du cabinet; dans les cinq pour cent restants, les renseignements n'existent pas. Dans huit pour cent des cas, les requérants n'ont pas fourni assez de renseignements pour qu'on accède à leur demande, il a été impossible de s'occuper de la demande, on a dû la transférer ou elle a été abandonnée.

Ces catégories n'ont guère changé depuis l'adoption de la *Loi sur la protection des renseignements personnels*.

Principaux ministères auxquels on s'adresse

La Défense nationale reste en tête du peloton, semant loin derrière les autres ministères pour le nombre de demandes reçues — presque 73 000 à la fin de 1987 — et maintient sa position depuis l'adoption du programme.

Viennent ensuite, par ordre d'importance décroissante, le Service correctionnel du Canada, 27 899; les Archives nationales, 25 964; la GRC, 11 111; et Emploi et Immigration Canada, 9 719.

Plaintes réglées par institution, motifs et résultats

Ministère	Genre	Nombre (Total)	Justifée (Total)	Rejetee (Total)	Abandonnee (Total)
Affaires des anciens combattants	**Retard**	**8**	**—**	**8**	**—**
Affaires exterieures	Acces Util. abus	4 1(5)	— 1	3 1	1 —
Affaires indiennes et du Nord Canada	**Accès** **Util. abus.**	**1** **1(2)**	**—** **1**	**1** **—**	**—** **—**
Agriculture Canada	Acces	6	—	6	—
Approvisionnements et Services Canada	**Accès**	**1**	**—**	**1**	**—**
Archives Publiques	Accès Correction	11 2(13)	4 —(4)	7 2(9)	— —
Banque du Canada	**Accès**	**1**	**—**	**1**	**—**
Bureau du Conseil prive	Acces Util. abus	10 1(11)	— —	10 1(11)	— —
Commission canadienne des droits de la personne	**Accès** **Util. abus.**	**4** **1(5)**	**1** **—(1)**	**3** **1(4)**	**0** **—**
Commission canadienne des transports	Accès	3	—	3	—
Commission d'appel de l'immigration	**Accès** **Util. abus.**	**1** **1(2)**	**1** **—**	**—** **1**	**—** **—**
Commission de la Fonction publique	Accès Correction	20 1(21)	— —	20 1(21)	— —
Commission nationale des libération conditionnelles	**Accès** **Correction** **Retard**	**11** **1** **3(15)**	**—** **—** **—**	**9** **1** **3**	**2** **—** **—**
Communications	Acces	1	1	—	—
Conseil canadien des relations au travail	**Accès**	**6**	**—**	**6**	**—**
Conseil du Trésor du Canada	Acces Util. abus	1 2(3)	— —	1 2(3)	— —

Plaintes réglées par institution, motifs et résultats (suite)

Ministère	Genre	Nombre (Total)	Jusitifée (Total)	Rejetée (Total)	Abandonnée (Total)
Corporation commerciale canadienne	Accès	1	1	—	—
Défense nationale	Accès	6	2	4	—
	Util. abus	4	—	4	—
	Retard	32	22	10	—
	Collecte etc.	1(43)	—(24)	1(19)	—
Emploi et Immigration Canada	Accès	62	11	49	2
	Util. abus	4	—	4	—
	Retard	25	20	5	—
	Collecte etc.	5(96)	1(32)	3(61)	1(3)
Environnement Canada	Accès	2	—	2	—
Gendarmerie royale du Canada	Accès	71	6	64	—
	Util. abus	7	—	7	—
	Correction	7	1	6	—
	Retard	13	5	8	—
	Langue	1	—	1	—
	Collecte etc.	1(100)	—(12)	1(87)	—(1)
Justice Canada Ministère de la	Accès	9	1	8	—
	Retard	2(11)	—(1)	2(10)	—
Office nationale de l'énergie	Accès	1	—	1	—
Postes Canada	Accès	23	4	1	—
	Util. abus	2	1	19	—
	Correction	1	—	1	—
	Retard	1	—	1	—
	Collecte etc.	3(30)	—(5)	3(25)	—
Ports Canada	Retard	4	4	—	—
Revenu Canada, Douanes et Accise	Accès	5	2	3	—
	Util. abus	2	—	1	1
	Correction	1	—	1	—
	Retard	2(10)	1(3)	1(6)	—(1)
Revenu Canada, Impôt	Accès	12	2	10	—
	Util. abus	1	1	—	—
	Retard	3	—	3	—
	Collecte etc.	2(18)	—(3)	2(15)	—

Plaintes réglées par institution, motifs et résultats (suite)

Ministère	Genre	Nombre (Total)	Jusitifée (Total)	Rejetee (Total)	Abandonnée (Total)
Santé et Bien-être social	**Accès**	**9**	**3**	**6**	**—**
Service canadien du renseignement de sécurité	Accès Retard	20 3(23)	1 —(1)	19 3(22)	— —
Service correctionnel Canada	**Accès** **Util. abus.** **Correction** **Retard** **Langue** **Collecte etc.**	**104** **7** **6** **39** **9** **5(170)**	**12** **—** **1** **33** **1** **—(47)**	**88** **7** **5** **5** **8** **5(118)**	**4** **—** **—** **1** **—** **—(5)**
Societe pour l'expansion des exportations	Acces	1	—	1	—
Soliciteur général Canada	**Accès** **Correction**	**4** **1(5)**	**—** **—**	**4** **1(5)**	**—** **—**
Statistiques Canada	Retard Langue	1 1(2)	— —	1 1(2)	— —
Transports Canada	**Accès** **Correction** **Retard**	**3** **2** **3(8)**	**—** **—** **2(2)**	**3** **2** **1(6)**	**—** **—** **—**
Travail Canada	Accès	8	1	7	—
Travaux publics Canada	**Accès** **Util. abus.**	**2** **2(4)**	**1** **1(2)**	**1** **1(2)**	**—** **—**
Total		661	155	492	14

Origine des plaintes réglées par province et territoire	
Terre-Neuve	3
Île-du-Prince-Édouard	2
Nouvelle-Écosse	13
Nouveau-Brunswick	8
Québec	219
Région de la Capitale nationale	
Québec	4
Région de la Capitale nationale	
Ontario	107
Ontario	131
Manitoba	30
Saskatchewan	25
Alberta	57
Colombie-Britannique	53
Territoires du Nord-Ouest	4
Yukon	1
Hors Canada	4
Total	**661**

PLAINTES

Usage commercial des données

La divulgation de listes de fonctionnaires ministériels à des fins commerciales est une question controversée qui a attiré notre attention pendant l'année.

La meilleure façon d'expliquer le problème est de parler des plaintes déposées par plusieurs officiers militaires selon lesquels la divulgation d'une liste d'employés de la Défense nationale à un homme d'Ottawa enfreignait la *Loi sur la protection des renseignements personnels*. Les plaignants ont soupçonné la vente des listes quand ils ont commencé à être sollicités par un promoteur immobilier local.

Invoquant la *Loi sur l'accès à l'information*, l'homme en question a demandé la liste de tous les employés civils et militaires de la Région de la capitale nationale « dont l'échelle salariale est égale ou supérieure à 42 000 $ par an », avec leur « nom, rang, classification, niveau, adresse au bureau, direction ou unité ».

Normalement, on ne peut divulguer des renseignements personnels en vertu de la *Loi sur l'accès à l'information*. L'agent de la compagnie lui-même s'est demandé si l'obtention de ces renseignements n'était pas contraire à la *Loi sur la protection des renseignements personnels*, mais la *Loi* est claire : les renseignements relatifs aux postes, aux fonctions et à l'échelle salariale des fonctionnaires, à leur titre, à leur adresse et à leur numéro de téléphone professionnels ne sont pas « personnels ». Cette exception énoncée dans la *Loi* établit le droit légal qu'a le public de savoir qui est payé sur les fonds publics, et à quelle fin. L'enquête a donc entièrement porté sur l'interprétation de la définition des renseignements personnels à l'égard des fonctionnaires fédéraux.

Même dilemme à la Gendarmerie

La question de la sécurité est revenue sur le tapis lors de plaintes similaires déposées par des membres de la GRC. Le Commissaire a conclu que le ministère de la Défense nationale était obligé de communiquer les renseignements, et qu'il n'avait d'autre alternative que de rejeter les plaintes, parce que le texte de la *Loi* est clair. Mais la question est préoccupante. Les fonctionnaires fédéraux ne devraient pas devenir la cible de sollicitations répétées pour divers biens et services. Les auteurs de la *Loi sur la protection des renseignements personnels* ne pouvaient avoir prévu cette éventualité.

En outre, la communication du nom du personnel et des militaires peut poser un problème de sécurité, car beaucoup d'employés travaillent à des postes délicats et ne figurent même pas dans les répertoires du ministère.

Après son enquête, le Commissaire a écrit au sous-ministre de la Défense nationale pour lui manifester son inquiétude que le « personnel employé dans des secteurs à haute sécurité particulièrement délicats ne soit identifié par des intérêts hostiles ». La manipulation de certaines listes informatisées pourrait permettre de déterminer comment le ministère de la Défense « affecte son personnel par grade et par endroit, révélant de ce fait ses priorités militaires ou dans le domaine du renseignement pour ses activités et ses projets ». Le Commissaire a demandé au ministère d'appuyer une modification de la *Loi sur la protection des renseignements personnels* pour remédier à cette lacune. (Voir aussi la plainte suivante).

Ce corps policier avait donné suite à une requête presque identique à celle de la Défense nationale, mais un représentant des relations avec le personnel de la GRC a fait part au Commissaire de « sa vive inquiétude » que les renseignements « ne tombent pas en de mauvaises mains ».

La lettre poursuivait ainsi :

> « La nature même du travail policier expose ses membres à des représailles possibles par...des terroristes, des vendeurs de drogue et des ennemis de la police dont les exploits remplissent quotidiennement les journaux. Tout policier qui travaille, ou a travaillé, dans la répression de la drogue ou du terrorisme confirmera que des renseignements comme le lieu de travail et le numéro de téléphone pourraient, aux mains de criminels, entraver les opérations policières et faire courir des risques aux policiers et à leur famille ».

Le Commissaire a réitéré sa conviction qu'« il faut mieux protéger les renseignements que détient le gouvernement sur ses fonctionnaires ». Il a recommandé que le Parlement modifie le texte de l'article afin de préciser la nature publique ou non de ces renseignements. Tant que la définition n'aura pas été resserrée, les ministères devraient pouvoir cacher certains renseignements professionnels sur les fonctionnaires quand leur sécurité est en jeu.

Obtention d'un classement dans la liste de mérite

Un officier des Forces armées s'est plaint au Commissaire de ce que le ministère de la Défense nationale refusait de lui révéler sa place exacte sur une liste de promotions. Ces listes sont faites annuellement par des comités de mérite chargés d'étudier les dossiers des membres admissibles dans chaque grade et groupe professionnel.

La Défense nationale a bien remis à l'officier un imprimé d'ordinateur quasi-vierge contenant des titres de colonnes et son nom, en tout et pour tout, sur une ligne, sans classement. Le ministère, lui a-t-on dit, a cessé de numéroter l'ordre de promotion en 1978, et en l'absence d'indications à côté des noms, on ne peut fournir le renseignement, puisqu'il « n'est pas consigné ».

En qualité d'ancien gestionnaire en carrières, le plaignant a dit qu'il savait que les cadres numérotaient souvent les listes et qu'on lui avait même dit sa place tous les ans de 1980 à 1985. Il pensait aussi que le numéro de page de la copie était inexact.

La Défense nationale a reconnu que certains militaires avaient été informés de leur classement dans le passé, mais comme cela s'est su, les demandes ont afflué et il a fallu consacrer trop de temps pour y répondre, si bien que cette pratique a été interrompue. Le ministère a dit à l'enquêteur du Commissariat que, même s'il pouvait trouver la place d'un officier en parcourant la liste, il n'était pas tenu de le faire, parce que ce ne sont pas des renseignements « sous une forme ou un support quelconque », donc pas reconnus comme renseignements personnels en vertu de la *Loi sur la protection des renseignements personnels*. (Le personnel a réitéré que le numéro de page était exact.)

L'enquêteur a confirmé que la liste était dressée « par ordre de mérite » et qu'elle servait à des décisions administratives sur les individus tels que l'avancement, la participation à des cours et l'aptitude à occuper un emploi.

Il est d'avis que la place d'un officier sur la liste entre dans la définition des renseignements personnels de la *Loi* qui vise « tout numéro ou symbole, ou toute autre indication identificatrice, qui lui est propre ».

Les parties se sont renvoyées la balle pendant plusieurs mois. Après avoir examiné la liste des promotions, l'enquêteur a attesté l'absence de classement numérique et a constaté que le numéro de la page était erroné, comme le soutenait le plaignant. L'erreur a été corrigée.

Le Commissaire a prévenu le sous-ministre d'une conclusion préliminaire voulant que la plainte était justifiée parce que la liste contenait deux éléments d'information sur l'individu : son nom sur la liste, et sa place par rapport aux autres. Il a écrit : « ...en refusant de communiquer la place exacte de X sur la liste pour la simple raison qu'aucun numéro n'y correspond, le ministère refuse certainement à X l'accès à un élément des renseignements de la liste le concernant ».

En septembre 1987, le Chef de l'état-major de la Défense a avisé le Commissaire que, après examen, le ministère avait changé sa politique.

« Les comités 1987 ajouteront un numéro de classement aux listes de mérite... » a écrit le Chef. À partir du 1er janvier 1988, les requérants recevront leur classement et les effectifs totaux examinés par le comité.

La lettre indiquait aussi la place du plaignant dans la liste 1987 de promotion.

L'assurance-chômage doit limiter ses questions sur les retraites

Un Ontarien s'est plaint des questions qu'on lui a posées sur sa retraite lorsqu'il a sollicité des prestations d'assurance-chômage.

Ce document, appelé « questionnaire de recherche des faits » demandait au requérant d'inscrire le montant de sa retraite, son origine, les modalités de paiement, si des sommes reçues avaient été converties en RÉER, en rentes ou placées dans « tout autre programme, compte ou régime d'épargnes ou d'investissement ».

Pendant l'enquête, le personnel d'Emploi et Immigration Canada (EIC) a indiqué qu'une modification de la *Loi sur l'assurance-chômage* datant de 1986 prévoyait que les prestations d'assurance-chômage des requérants bénéficiaires d'une retraite pouvaient être réduites. Le questionnaire avait donc pour objet de déterminer si les requérants avaient une retraite. Comme les renseignements concernaient l'administration du programme d'assurance-chômage, ils étaient légitimes en vertu de la *Loi sur la protection des renseignements personnels*.

Le Commissaire a reconnu que cette explication aurait été valable si les questions avaient visé la période de chômage du requérant. Mais elles étaient ouvertes, ce qui poussait les intéressés à révéler des renseignements sur des bénéfices pouvant n'être versés que beaucoup plus tard. Dans ces conditions, le Commissaire a fait savoir à EIC que la collecte de ces renseignements lui paraissait prématurée.

Le ministère a accepté d'ajouter une note au bas du questionnaire, en limitant à la période de chômage les questions sur les prestations de retraite. Il a ensuite annoncé qu'il allait établir un nouveau questionnaire national, sans note.

Après trois mois de pourparlers, EIC a accepté d'ajouter l'énoncé restrictif dans la nouvelle formule. Malheureusement, l'homme dont la plainte a infléchi la politique est parti sans laisser d'adresse. Il n'a jamais appris la bonne nouvelle.

Renseignements médicaux — Société canadienne des postes

Un employé des Postes s'est plaint de ce que la Société ait communiqué mal à-propos des renseignements à son médecin, qu'elle ait obtenu des renseignements personnels du médecin sans son accord, et qu'elle ait utilisé un dossier médical produit pendant une audience de rémunération pour empêcher son retour au travail.

L'enquête a confirmé que la Société canadienne des postes s'est servi du dossier médical de l'audience pour empêcher le plaignant de reprendre son service. Le fichier où se trouvait le rapport (« Hygiène et sécurité au travail ») est présenté comme contenant des renseignements utilisés « pour déterminer les conditions dans lesquelles des employés...affligés de maladies ou d'invalidités déclarées peuvent continuer à travailler... ». Le Commissaire a conclu que la Société canadienne des postes n'avait pas fait mauvais usage des renseignements.

Le Commissariat a appris au cours de l'enquête que la Société avait obtenu les renseignements du médecin sans l'autorisation de l'employé, mais que la demande avait été faite avant l'adoption de la *Loi sur la protection des renseignements personnels*, et qu'elle n'enfreignait donc pas la *Loi*. Il a aussi constaté qu'une copie de la correspondance envoyée par la Société au plaignant, avec des renseignements personnels, avait été communiquée abusivement au médecin. La Société canadienne des postes veillera à ce que la situation ne se reproduise plus.

Congés et diagnostics médicaux

Le Commissaire a reçu deux plaintes contre des ministères qui demandaient des renseignements médicaux détaillés à des employés en congé de maladie.

Dans un cas, déjà invoqué pour montrer la nécessité de protéger le droit à la vie privée au travail, un surveillant du ministère des Communications (MDC), après avoir refusé la déclaration normale de congé de maladie et le certificat médical d'un subordonné, a insisté pour connaître les raisons médicales qui l'avaient empêché de travailler. Cet employé s'était longuement absenté pour des raisons de santé.

L'employé a refusé de renseigner son supérieur. Il a cependant accepté de se faire examiner par un médecin de Santé nationale et Bien-être social qui, s'il a trouvé l'employé en bonne santé, n'a pu justifier ces absences répétées parce qu'on ne l'a pas laissé parler au médecin soignant.

Quand le ministère a refusé de payer le congé de maladie, le fonctionnaire s'est plaint en arguant qu'il était contraire à la *Loi sur la protection des renseignements personnels* d'exiger la communication du diagnostic.

Le ministère a rétorqué qu'il avait le droit de savoir vu les nombreux congés de maladie de l'employé, qu'il se préoccupait de la santé et de la sécurité de l'intéressé et de ses collègues, et des répercussions des cas d'invalidité à long terme. Le MDC a aussi cité la convention collective et la décision d'arbitrage d'un grief pour appuyer sa thèse.

Le Commissaire a reconnu qu'il était légitime de demander une preuve d'inaptitude au travail pour des raisons médicales avant de payer un congé de maladie. Les employeurs peuvent faire effectuer un contrôle médical par un médecin de leur choix mais, a-t-il dit, « je n'estime pas nécessaire que l'employeur sache la nature de la maladie ».

Après cette plainte, le ministère a changé de politique. À l'avenir, on ne demandera plus de précisions sur la santé des employés; on fera vérifier le cas échéant l'aptitude au travail par un médecin de Santé nationale et Bien-être social; le diagnostic ne sera pas divulgué. Le ministère des Communications a fini par payer le congé de maladie du plaignant.

Retrait du diagnostic d'un dossier

Une femme de Québec s'est plainte de ce que son employeur (Emploi et Immigration Canada) ait demandé, sans son consentement, des renseignements médicaux après qu'elle eut remis un certificat d'invalidité. Ces renseignements ont été ensuite versés à son dossier au service du personnel.

Le ministère a expliqué que les cadres contactent souvent les médecins traitants pour savoir le travail que peut fournir un employé ayant des problèmes de santé, mais sans demander des précisions sur leur état. C'est plus rapide que d'attendre que les fonctionnaires obtiennent eux-mêmes les renseignements et, selon EIC, la plaignante savait qu'on téléphonerait à son médecin, qu'elle le veuille ou non.

Le Commissaire a conclu que, dans un cas semblable, le ministère doit recueillir l'information directement auprès de l'employé(e) ou solliciter l'autorisation de l'intéressé(e) avant de joindre le médecin traitant. Ensuite, l'employeur doit se contenter de demander la durée prévue de cet état de santé et les éventuelles précautions à prendre au retour de l'employé(e).

Après des mois de tractations, Emploi et Immigration Canada a accepté de supprimer le diagnostic médical du dossier.

Comme le Commissaire est persuadé que ce cas n'est pas isolé, il a incité le Conseil du Trésor à émettre des directives conformes à la *Loi sur la protection des renseignements personnels* pour l'ensemble de l'Administration fédérale.

Refus de communication à la Police

Un détenu s'est plaint en déplorant que le Service correctionnel du Canada ait fait un mauvais usage de renseignements personnels en communiquant son « dossier pénitentiaire » à la police municipale. Il a prétendu que la police a alors remis ce dossier à un procureur et à un psychiatre de la Couronne avant de le remettre à son avocat.

L'enquêteur du Commissaire à la protection de la vie privée n'a pas trouvé la preuve que les dossiers personnels étaient passés de mains en mains. Le plaignant a pourtant produit une page copiée d'une transcription du tribunal où le psychiatre mentionnait les tests et les dossiers sur lesquels il avait fondé son évaluation du détenu. L'une des pièces était intitulée « rapports de police et dossiers du service pénitentiaire ».

Même si le psychiatre a eu accès aux dossiers, ce semble un usage compatible, étant donné que l'audience avait pour objet de juger si le détenu était un contrevenant dangereux. Rien n'a prouvé que les renseignements aient été remis à la police.

À défaut de preuves que des renseignements personnels avaient été employés à tort ou de façon inopportune, le Commissaire a rejeté la plainte.

Les syndicats contre les enquêtes de sécurité

Trois syndicats de la fonction publique se sont plaints des enquêtes de sécurité et de fiabilité instaurées par Revenu Canada. Leurs membres estimaient en effet « illégale » la collecte des antécédents judiciaires, des opérations financières et des empreintes digitales, et ils ont demandé au Commissaire de faire enquête, en particulier sur la politique de sélection du personnel appliquée par Revenu Canada (Impôt).

Après le vol de microfiches sur les contribuables (Rapport annuel 1986 — 1987, page 11), le ministre du Revenu national a immédiatement ordonné la mise en place à l'Impôt de la nouvelle politique de sécurité applicable à toute l'Administration fédérale. Les vérifications de base prévues à cet effet comprennent le contrôle de la formation et de l'expérience professionnelle, des renseignements sur l'emploi, des évaluations de rendement et de personnalité et une vérification des fichiers nominatifs des casiers judiciaires. L'enquête de sécurité « approfondie » comporte en outre le relevé des empreintes digitales et une vérification du crédit.

Le Commissaire a jugé que le Conseil du Trésor avait le droit (et même le devoir) d'évaluer la fidélité et la loyauté des fonctionnaires pour prévenir l'emploi abusif ou la communication de renseignements personnels touchant les contribuables.

Il craint pourtant toujours que des tiers ne demandent à voir des dossiers de sécurité individuels au nom de la *Loi sur l'accès à l'information*, puisque les renseignements personnels des fonctionnaires sont mal protégés. Après des pourparlers, déclenchés par une plainte similaire contre le code gouvernemental relatif aux conflits d'intérêts, le Conseil du Trésor a promis de demander au Parlement de modifier la *Loi sur la protection des renseignements personnels* afin de limiter l'accès des renseignements personnels des fonctionnaires aux noms, aux échelles salariales, aux titres, aux postes, aux fonctions et aux adresses de bureau.

Le Conseil du Trésor a accepté la recommandation du Commissaire que les sous-ministres soient autorisés à décider du bien-fondé d'une vérification des empreintes digitales et du crédit, et pour quels employés. La politique a été changée.

Un vérificateur fiscal obtient les notes d'une réunion

Un vérificateur fiscal de Revenu Canada s'est plaint du Commissaire quand le ministère a soustrait des éléments d'une lettre qui l'accusait de conflit d'intérêts. Il a jugé « dénuées de sens » les pages « censurées » qu'on lui avait remises.

Un homme avait écrit au ministre du Revenu en alléguant que le vérificateur en question (premier mari de sa femme) profitait de sa situation pour faire pencher la balance de son côté dans un différend juridique avec la femme. En outre, poursuivait l'homme, le vérificateur s'en était pris récemment à l'un de ses collègues de travail qui avait omis de déclarer des revenus, laissant entendre que les incidents étaient reliés. Les enquêtes internes du ministère n'ont rien révélé de répréhensible de la part du vérificateur.

Un enquêteur a persuadé le ministère de communiquer plus d'éléments de la lettre originale. Mais comme une partie importante des données inconsultables consistaient en renseignements personnels sur quelqu'un d'autre, la dispense était justifiée.

Dans l'intervalle, le plaignant a ré-écrit au ministère en exprimant la crainte qu'une enquête interne ne produise d'autres documents que ceux qui étaient en sa possession. Lorsqu'il a rencontré le coordonnateur ministériel de la protection des renseignements personnels, le vérificateur a demandé les éventuelles notes personnelles prises par les gestionnaires pendant les entrevues de l'enquête interne sur le conflit d'intérêts et le dossier de l'enquête. Il a aussi demandé à examiner le dossier fiscal de l'employé surpris à frauder le fisc.

L'enquêteur a négocié la divulgation de quelques notes de réunions et le compte rendu d'une conversation téléphonique avec la personne qui avait allégué l'existence d'un conflit d'intérêts. Mais il a confirmé qu'il n'y avait pas d'autres notes personnelles, pas de dossier d'enquête ni d'allusion au plaignant dans la lettre de réponse du ministre à la plainte originale ou dans le dossier fiscal du collègue de bureau.

Le Commissaire a maintenu la plainte parce que le ministère n'avait pas fourni tous les documents en réponse à la première demande. Le requérant est maintenant en possession des documents auxquels il avait droit.

La GRC effectue une correction, en refuse une autre

Un Manitobain s'est plaint de ce que la GRC ait rejeté une demande visant à corriger les renseignements factuels d'un dossier obtenu à la suite d'une requête aux termes de la *Loi sur la protection des renseignements personnels*.

L'enquêteur a constaté que la GRC avait accepté un correctif, mais en avait refusé un autre pour la raison qu'un agent de la GRC avait donné une autre version de l'incident. Les commentaires du plaignant ont été versés au dossier.

Dans la lettre qu'il a écrite au plaignant, le Commissaire a expliqué qu'il n'existait pas de méthode précise de trancher les différends sur les divergences de perception d'un incident. Mais comme la version du plaignant figure maintenant dans le dossier, la décision de la GRC était acceptable.

Un consentement permet une divulgation

Un employé d'Emploi et Immigration Canada (EIC) accusé de conflit d'intérêts au moment d'un recrutement a prétendu que le ministère ne lui avait pas fourni toute la documentation réclamée, que EIC avait recueilli des renseignements inopportuns pendant l'enquête et avait tardé à répondre à sa demande.

Emploi et Immigration Canada n'avait effectivement pas donné suite à la note de service demandant copie de documents de l'enquête, mais pour trois raisons : le plaignant n'avait pas utilisé le formulaire pertinent; il n'avait pas invoqué la *Loi sur la protection des renseignements personnels* et n'avait pas envoyé la demande au bureau de la protection des renseignements. Techniquement, ce n'était pas une demande officielle liée à la protection des renseignements personnels et le ministère n'était pas tenu de répondre.

Quand il a reçu une requête en bonne et due forme, Emploi et Immigration a prorogé le délai jusqu'au maximum de soixante jours pour ne pas « entraver de façon sérieuse le fonctionnement de l'institution ». Comme le personnel devait manipuler un nombre important de documents, le délai était raisonnable.

À la réception des documents, le requérant s'est aperçu que des renseignements avaient été soustraits parce qu'ils concernaient une tierce personne (surtout la personne engagée). Par ailleurs, il s'attendait à recevoir les notes prises par son supérieur le jour de leur rencontre, des documents de l'unité de relations de travail, les entrevues avec les membres du personnel sur le recrutement et la correspondance pertinente échangée avec le ministre. Comme tout manquait, il a déposé une plainte.

L'enquêteur a appris que les notes manuscrites du supérieur avaient été détruites après la rédaction du rapport. Il n'y avait pas de document à l'unité des relations de travail et les comptes rendus des entrevues avec les autres personnes étaient inconsultables à juste titre. La correspondance du ministre, qui avait été oubliée, a été communiquée. Et après que le plaignant eut obtenu le consentement d'une tierce partie, Emploi et Immigration a également divulgué ce renseignement.

Le Commissaire a rejeté la plainte que EIC avait recueilli des renseignements impropres. Le ministère avait certes fait des enquêtes à l'extérieur, dont des entrevues avec les voisins du plaignant, mais la jurisprudence donne une grande latitude aux employeurs de s'assurer de la conduite de leurs employés.

Un statut litigieux entrave l'accès à l'information

Un mari et sa femme se sont plaints de ce qu'un conseiller en immigration chargé de les représenter se soit vu refuser l'accès à leur dossier d'immigration parce que, selon Emploi et Immigration Canada, le couple ne remplissait pas les exigences de la *Loi sur la protection des renseignements personnels*. Il faut en effet être citoyen canadien ou résident permanent pour déposer une requête.

Les deux plaignants avaient obtenu leur statut d'immigrants reçus au début de 1985. Mais ils sont partis en vacances à l'étranger en 1986 et, à leur retour, les agents de l'immigration ont cru que le couple avait renoncé à son statut au Canada et le lui ont dit. Les intéressés ont soutenu qu'aucun des deux n'avait été absent du pays du maximum de 183 jours autorisé et qu'aucun arbitre de l'immigration n'avait annulé leur statut.

L'enquêteur a examiné la requête avec le personnel de EIC, qui a proposé d'étudier la demande d'après la *Loi sur l'accès à l'information*, ce qui aurait permis au conseiller en immigration de demander les renseignements moyennant le consentement des intéressés.

Le conseiller a refusé, parce que cela serait revenu, selon lui, à admettre que ses clients n'étaient pas des résidents permanents. Tandis que les discussions se poursuivaient au ministère, le problème de l'immigration a été résolu et le couple a retiré sa plainte.

Les employés d'un entrepreneur sont protégés

Un homme d'Ottawa a déclaré au Commissaire que les Affaires extérieures lui avaient remis le nom d'une entreprise de travail temporaire qui fait affaire avec le ministère et, par surcroît, la liste des employés qui fournissaient les services.

C'est à son avis une violation de la *Loi sur la protection des renseignements personnels* et il a déposé une plainte. En effet, seuls peuvent être communiqués les noms des signataires de contrats de service avec le gouvernement, parce que ce ne sont pas des « renseignements personnels ». Dans ce cas, le contrat avait été conclu avec l'organisme, et le plaignant trouvait que le nom des individus devait être protégé.

Selon le plaignant, les ministères n'appliquent pas une politique uniforme et plusieurs ne divulguent que le nom de l'entreprise, s'abstenant de donner celui des employés. Il faut harmoniser la pratique, estime-t-il, et les Commissaires à l'information et à la protection de la vie privée devraient donner des conseils.

À l'issue de son enquête, le Commissaire à la protection de la vie privée a jugé que la plainte était fondée. Les employés d'une entreprise qui fournit des services contractuels au gouvernement fédéral ne sont pas eux-mêmes des fonctionnaires. Ils ont donc le droit à la protection des renseignements personnels les concernant.

Le même requérant a ensuite demandé au ministère des Affaires extérieures quelle était la cote de sécurité aux emplois de ces individus. Le ministère a refusé de répondre parce que les individus avaient déjà été désignés. Le requérant s'est plaint au Commissaire à l'information qu'on lui refusait l'accès à l'information. L'affaire a été portée devant la Cour fédérale.

Direction de l'observation

« Pour le contrôle d'application..., le Commissaire à la protection de la vie privée peut, à son appréciation, tenir des enquêtes quant aux renseignements personnels qui relèvent des institutions fédérales »

Article 37 de la Loi sur la protection des renseignements personnels

Les enquêteurs de la Direction de l'observation ont planifié et effectué cette année pour la première fois plusieurs vérifications à l'aide du modèle élaboré l'an dernier en fonction des risques. Comme la série de documents perdus évoquée dans le rapport de 1986 — 1987 a cessé, le personnel a pu orienter ses efforts sur l'observation de la *Loi* dans quatre ministères, choisis par la direction, dans les administrations considérées comme « à haut risque ».

L'enquête effectuée à Transports Canada (TC), au Service correctionnel du Canada (SCC), à Environnement Canada (EC) et à Agriculture Canada (AC) a permis au Commissariat de faire ses premières armes dans de gros ministères qui possèdent de nombreux bureaux et un vaste assortiment de fichiers de renseignements personnels. Il avait seulement fait auparavant un premier essai de vérification à Pêches et Océans et dans les fichiers inconsultables de huit administrations.

La direction avait alors surestimé les ressources nécessaires à un examen complet puisque, par nature, les dossiers des fichiers inconsultables sont particulièrement délicats et plus uniformes ou homogènes qu'ailleurs. Recueillis en fonction de paramètres précis et faisant l'objet d'un contrôle central (mais pas forcément conservés dans un endroit central), ils réservent peu de surprise.

Les autres fichiers de renseignements personnels ont en revanche forcé le Commissariat à repenser les enquêtes et les calendriers, et à élaborer de nouvelles méthodes, puisqu'il est vite apparu qu'on ne pouvait se contenter de vérifications de principe tel que prévu initialement.

Le Commissariat envoie généralement des équipes de deux à quatre agents qui visitent un certain nombre de services de l'administration centrale et plusieurs bureaux régionaux. Ces enquêteurs prélèvent au hasard quelques dossiers de certains fichiers et rencontrent les gestionnaires et le personnel qui utilisent les dossiers et les gèrent.

Les enquêteurs examinent :

* la collecte, l'usage, la divulgation, la conservation, le retrait et la sécurité des renseignements personnels du ministère;

* la valeur des lignes directrices internes et l'observation par le ministère de la politique et des directives de l'organisme central en matière de renseignements personnels;

* l'exactitude et le caractère exhaustif du contenu du Répertoire de renseignements personnels du ministère;

* la connaissance qu'a le personnel de la *Loi sur la protection des renseignements personnels* et de ses effets sur le traitement de ces renseignements;

* l'accès des particuliers aux renseignements personnels les concernant;

* la délégation des pouvoirs effectuée par le (la) responsable du ministère.

Une fois la vérification terminée, les enquêteurs discutent avec les gestionnaires des lacunes relevées. Le ministère reçoit un projet de rapport pour examen, puis un rapport final. Selon la pratique courante, les rapports ne portent que sur les points à corriger.

Conclusions :

Bien que les quatre ministères soient fort différents, nous avons été surpris de parvenir à des conclusions assez semblables. Par exemple :

* exception faite du personnel des sections chargées de protéger les renseignements personnels, peu d'employés connaissaient les effets de la *Loi sur la protection des renseignements personnels* sur l'utilisation quotidienne des renseignements personnels à l'égard d'un employé ou d'un client :

* exception faite du SCC, la sécurité matérielle des renseignements personnels était souvent insuffisante;

* certains dossiers contenant des renseignements personnels n'avaient pas été identifiés et décrits dans le Répertoire;

* quelques inscriptions des fichiers de renseignements ne mentionnaient pas les « usages compatibles » des renseignements que le ministère faisait couramment.

Les enquêteurs ont constaté que certaines lignes directrices de quelques ministères en matière de renseignements personnels s'écartaient de la *Loi sur la protection des renseignements personnels*, mais la plupart des cas vont être corrigés.

Le personnel du Commissariat a aussi fréquemment remarqué la prolifération des copies de travail de dossiers du personnel. Bien que la *Loi* ne prévoie rien expressément à ce sujet, le Commissariat demande aux ministères d'examiner toutes leurs copies lorsqu'ils répondent à une demande de communication, et de veiller à ce que toutes les copies respectent la *Loi*. L'usage croissant des ordinateurs personnels ne facilitent pas la tâche.

Une dernière constatation : les quatre ministères ont étroitement collaboré avec les enquêteurs. La plupart des employés ont été intéressés par l'enquête et en ont profité pour se renseigner sur la *Loi*.

Voici un résumé des rapports établis à l'issue de ces vérifications.

LES VÉRIFICATIONS

Environnement Canada

Les trois principales composantes d'Environnement Canada, les Services de l'environnement atmosphérique (le bureau de météorologie), le Service de la conservation et de la protection, le Programme Parcs, sont disséminées dans tout le pays. Le ministère recueille un nombre limité de renseignements personnels sur le grand public, qui n'ont généralement rien de délicat. Il possède ainsi des fichiers sur les permis délivrés en vertu de la *Loi sur la Convention concernant les oiseaux migrateurs* et de la *Loi sur l'immersion de déchets en mer*, sur les permis de chasse au canard et de pêche ainsi que sur les sondages effectués auprès des visiteurs des parcs nationaux. La majorité des renseignements personnels d'Environnement Canada vise ses propres employés.

L'équipe de vérification s'est rendue dans les bureaux d'Environnement Canada de Sackville (Nouveau-Brunswick), Dartmouth (Nouvelle-Écosse), Toronto (Ontario), Calgary (Alberta) et à l'administration centrale de Hull (Québec).

Constatations :

* la plupart des employés d'Environnement Canada ne savaient pas grand-chose de la *Loi sur la protection des renseignements personnels*, de son application et de ses effets pour leur travail. Les directives internes étaient souvent inadéquates, inexactes et ignorées;

* les calendriers de retrait n'étaient pas respectés, si bien que les renseignements étaient soit gardés plus que nécessaire, soit moins des deux ans réglementaires;

* certains dossiers du personnel étaient entreposés dans des endroits peu sûrs;

* les dossiers du personnel concernant les particuliers ayant des contrats de services individuels, les bénévoles et les candidatures d'emploi non sollicitées ne figuraient pas au Répertoire de renseignements personnels;

* les gestionnaires tenaient, dans tout le ministère, des systèmes de dossiers en double ou des dossiers privés contenant des renseignements personnels principalement extraits des dossiers du personnel, ce qui augmentait le risque de divulgation non autorisée, de déformation des renseignements et de refus de les communiquer;

* le fichier de la *Loi sur l'immersion de déchets en mer* ne contenait pas de renseignements personnels — les dossiers visaient des entreprises, des sociétés et diverses administrations fédérales. (On peut l'éliminer du Répertoire de renseignements personnels.)

Transports Canada

Transports Canada est l'un des plus gros ministères fédéraux, avec près de 22 000 fonctionnaires chargés de veiller à l'établissement et à l'exploitation d'un système national de transport sécuritaire et efficace. Il comprend cinq groupes : Gestion des aéroports, Aviation, Marine, Surface, Politiques et coordination. Les enquêteurs ont fait des vérifications à la Gestion des aéroports, à l'Aviation et à la Marine, à l'administration centrale et dans quelques bureaux régionaux.

Dans l'ensemble, les renseignements personnels sont bien protégés. Les employés veillent à empêcher des divulgations indues; un système intégré de gestion des dossiers désigne et enregistre la plupart des renseignements personnels. Nous avons regroupé les lacunes relevées dans les rubriques suivantes : Contenu des fichiers de renseignements personnels figurant au Répertoire de renseignements personnels, Protection des renseignements personnels, Conservation et retrait, Sécurité, Collecte et mise au courant des intéressés, Communication.

Dossiers d'aide aux employés : lors de la préparation de l'enquête, le Commissariat a désigné un groupe de dossiers à haut risque, ceux du Programme d'aide aux employés (PAE), qui renferment des détails personnels très délicats.

(Ce programme fournit orientation et aide aux employés fédéraux ayant des problèmes de santé ou de comportement comme l'alcoolisme.) Seul le personnel d'orientation peut consulter ces dossiers.

Le ministère hésitait, non sans raison, à montrer ses dossiers à des étrangers, même à un enquêteur chargé de la protection de la vie privée, une divulgation non autorisée pouvant causer des torts irréparables à l'intéressé. Le Commissariat a donc convenu avec Transports Canada d'envoyer un fonctionnaire supérieur examiner des dossiers pris au hasard afin de voir s'ils étaient bien gérés et suffisamment protégés. Les numéros d'identification personnels ont été cachés.

L'enquêteur a constaté que les dossiers, déjà anonymes, se trouvaient dans une armoire sous clé située dans un bureau fermé à clé, dans un immeuble inaccessible après les heures de travail. Rien ne lui a pas permis de croire qu'il y avait des communications indues, mais il a fait plusieurs recommandations pour améliorer la sécurité matérielle des dossiers.

Voici les lacunes recensées à Transports Canada.

Contenu du Répertoire de renseignements personnels : les enquêtes ont fait apparaître plusieurs carences, dont :

* le fichier « Politique et procédure de mise en application » (P-PU-015) contenait des dossiers sur les activités d'application à l'égard des détenteurs d'un document valide de l'aviation au lieu de porter sur les personnes « pas en possession » du document;

* la base de données visant la délivrance des licences d'aviation (P-PU-005) n'indiquait pas que son contenu pouvait être partagé avec le Bureau canadien de la sécurité aérienne ni que le dossier médical « C » faisait partie du fichier;

* le fichier des accidents d'automobiles, de bateaux, d'embarcations et d'avions (P-OE-908), enregistré comme fichier ayant trait au personnel, contenait beaucoup de renseignements sur des membres du public qui avaient fait des réclamations à propos d'accidents intervenus pendant qu'ils utilisaient les installations du ministère.

Protection des renseignements personnels : certains renseignements personnels n'étaient pas suffisamment protégés d'une divulgation à des particuliers non autorisés. On pouvait ainsi obtenir, par téléphone, des renseignements sur les détenteurs de licence d'aviation. Les enquêteurs ont trouvé des listes de déductions salariales appartenant à plusieurs employés dans des dossiers individuels du personnel et des renseignements délicats sur des employés (dans un dossier « Antécédents ») lors de leur évaluation.

Dans un bureau régional, les enquêteurs du Commissariat ont trouvé un fichier non officiel de 26 volumes renfermant des renseignements souvent délicats sur tout le personnel, avec les noms classés par ordre alphabétique. Les gestionnaires pouvaient se renseigner sur n'importe quel employé, pas seulement sur leurs subordonnés.

La sécurité était relâchée à certains endroits. Les enquêteurs ont ainsi trouvé : des disques d'ordinateur qui traînaient la nuit; une salle de dossiers en aire ouverte où les fichiers étaient rangés sur des rayonnages ouverts, juste en face de l'ascenseur; du personnel d'entretien ayant accès aux fichiers de licences, et des documents délicats à éliminer jetés avec les autres rebuts.

Conservation et retrait des dossiers : l'équipe de vérification a trouvé qu'un fichier de renseignements n'avait pas de calendrier de retrait; deux autres devaient être examinés afin d'envoyer les vieux dossiers aux Archives nationales pour destruction ou stockage à des fins historiques. Des dossiers régionaux temporaires placés dans un fichier de rapports d'accidents étaient détruits avant les deux ans réglementaires. Certains avaient beau être des doubles de rapports envoyés à l'administration centrale, ils contenaient des notes des enquêteurs sur les accidents et devraient être conservés.

Collecte de renseignements personnels et mise au courant des intéressés : selon la *Loi sur la protection des renseignements personnels*, les institutions du gouvernement doivent donner aux particuliers les raisons de la collecte des renseignements personnels, et les expliquer notamment dans les formules de demande. Mais les formules utilisées afin de délivrer diverses licences et permis d'aviation civile ne contiennent pas de précisions et il y a lieu de croire que les requérants n'ont jamais été informés des fins auxquelles les renseignements seraient utilisés.

Les enquêteurs ont découvert une collection de ce qui semblait être des renseignements inutiles. Les certificats médicaux des pilotes demandaient, par exemple, des renseignements sur l'éducation, tandis que d'autres voulaient le lieu de naissance des requérants.

Accès aux renseignements personnels : dans une région, les requérants désireux de consulter le fichier de licences d'aviation se sont vu refuser l'accès à leur dossier médical dans ce fichier s'ils ne l'avaient expressément demandé.

Agriculture Canada

Agriculture Canada emploie 13 000 personnes dans 11 directions qui administrent 40 lois différentes. Ses programmes vont du maintien de la productivité du secteur agro-alimentaire canadien à la protection du bétail et de la flore, y compris les forêts canadiennes.

La vérification a été effectuée à Moncton (Nouveau-Brunswick), Calgary (Alberta) et à l'administration centrale d'Ottawa-Hull.

Protection des renseignements personnels : les enquêteurs ont trouvé, dans des bureaux régionaux, plusieurs dossiers de travail du personnel qui contenaient des détails personnels délicats. D'autres dossiers comportaient des renseignements inutiles sur des tiers. À plusieurs endroits, des renseignements personnels n'étaient pas sous clé, dans des bureaux ouverts. Dans un cas, les dossiers ouverts avaient trait à des méfaits présumés.

On trouve fréquemment dans les bureaux régionaux des dossiers de travail du personnel conservés pour l'administration courante. Ils n'enfreignent pas forcément la *Loi* si ce sont des répliques exactes de dossiers officiels; seules sont autorisées à s'en servir les personnes qui doivent connaître ces renseignements. Ces dossiers sont revus quant un employé présente une demande d'accès en vertu de la *Loi*.

Divulgation indue : Agriculture Canada a signé en 1985 un protocole d'entente avec Douanes Canada et la GRC pour verser des rapports d'enquête à un fichier informatisé de la GRC. Ces trois organismes, la police et le service douanier des États-Unis partagent les renseignements.

De l'avis des enquêteurs, les communications étaient, à quelques exceptions près, sans rapport avec les fins initiales de la collecte, aussi ont-ils incité le ministère à cesser de divulguer des renseignements tant qu'il ne respecterait pas la *Loi sur la protection des renseignements personnels*. Le ministère devrait répondre seulement aux demandes écrites d'organismes d'enquête comme la GRC, et tenir un registre des divulgations pour l'examen du Commissaire à la protection de la vie privée.

Connaissance de la Loi sur la protection des renseignements personnels : peu de fonctionnaires connaissaient la *Loi*. Il pouvait en découler une mauvaise façon d'utiliser les renseignements personnels, en gardant, par exemple, indéfiniment des rapports sur les conflits d'intérêt concernant d'anciens employés.

Le ministère a accepté de supprimer des renseignements périmés sur un système et de modifier son nouveau système pour prévoir des dates de destruction des dossiers. Les problèmes créés par l'accord susmentionné conclu avec les Douanes et la GRC venaient d'un manque de sensibilisation à la *Loi*.

Le Service correctionnel du Canada

Le Service correctionnel du Canada comprend le Service pénitentiaire, chargé de la garde et du soin des détenus, et le Service national des libérations conditionnelles, qui surveille les détenus libérés sous condition ou placés sous surveillance obligatoire.

Compte tenu des exigences de leur emploi, les employés estiment que la sécurité, le secret et la protection des renseignements personnels font normalement partie de leur travail.

Nous avons néanmoins relevé quelques domaines qui pourraient être améliorés.

Contenu du Répertoire de renseignements personnels : les enquêteurs ont découvert des contenus inexacts ou incomplets dans le Répertoire; parfois aussi, la finalité de la collecte manquait de précision. Des dossiers contenaient des demandes de services de renseignements, des demandes du ministère, des enquêtes administratives, des dossiers de transfert de détenus — collectes de renseignements personnels qui ne figuraient pas au Répertoire.

En outre, 12 séries de dossiers portant sur des renseignements personnels étaient absentes du Répertoire, ce qui empêchait le public d'accéder aux renseignements et qui lui cachait l'ampleur de la collecte et ses fins. Autres conséquences possibles, ces dossiers n'étaient peut-être pas conservés pendant les deux ans réglementaires ou n'étaient pas réexaminés périodiquement pour être détruits.

Protection des renseignements personnels : les employés des régions de l'Ontario et du Québec ne pouvaient voir le dossier du personnel les concernant que s'ils en faisaient la demande à leur supérieur hiérarchique, et en sa présence. Certains bureaux de ces régions n'avaient pas de lignes de conduite pour l'élimination sécuritaire des rubans lisibles d'ordinateurs et de machines à écrire.

Les enquêteurs ont trouvé, à l'administration centrale nationale, des registres délicats d'octroi de pardon sur des rayonnages ouverts dans une aire de rangement du sous-sol. Quiconque avait accès à la pièce pouvait consulter les dossiers.

Droits d'accès : les détenus de l'Ontario qui demandaient l'accès au fichier de psychologie (CPS/P-PU-070) ne recevaient pas les données brutes de leurs tests. Le personnel de psychologie du Centre de psychiatrie régional de l'Ontario et l'établissement de Joyceville conservaient systématiquement les évaluations avant d'envoyer les dossiers à l'administration centrale, sans avoir prévenu le coordonnateur de la protection des renseignements personnels du ministère. On ne disait aux requérants ni les pièces qui manquaient ni qu'ils pouvaient déposer une plainte auprès du Commissaire à la protection de la vie privée.

Code d'usage et de divulgation : nous examinons en détail à la page 16 les problèmes que le Commissariat a rencontrés en ce qui a trait au code d'emploi et de divulgation du Service correctionnel.

Aviser le Commissaire

L'un des objets de la *Loi sur la protection des renseignements personnels* est d'empêcher la divulgation de renseignements personnels sur des individus. Mais il y a rarement des règles sans exceptions. La *Loi* prévoit donc des dérogations, notamment « pour des raisons d'intérêt public », pour se conformer à une autre loi du Parlement ou aux exigences d'une assignation à témoigner ou d'un mandat, pour répondre à une demande d'un organisme d'enquête déterminé ou dans le cas des archives publiques, pour dépôt.

Lorsque des ministères décident de communiquer des renseignements personnels, ou pour toute nouvelle utilisation « compatible » avec le but de la divulgation, ils doivent cependant donner un préavis au Commissaire à la protection de la vie privée, qui peut ainsi s'opposer aux communications lui paraissant dénuées de fondement et avertir les individus s'il le juge nécessaire.

Voici les avis que le Commissaire a reçus cette année :

Affaires des anciens combattants : communication du dossier médical d'un ancien combattant décédé au médecin de sa fille, pour rechercher la possibilité d'une maladie héréditaire.

— communication du dossier médical d'une personne décédée à un fils, pour traiter une maladie soupçonnée d'être héréditaire.

Affaires indiennes et du Grand Nord : confirmation du statut d'Indien inscrit d'un homme décédé, pour aider sa fille à obtenir le statut d'Indienne inscrite.

Commission nationale des libérations conditionnelles : communication de la décision de la Commission et des motifs de la décision à un député qui soupçonnait une allégation d'ingérence politique.

Défense nationale : communication de la déclaration sous serment du médecin traitant à la femme d'un homme dans le coma, pour lui permettre de gérer les affaires financières de la famille.

Gendarmerie royale du Canada : communication d'un rapport de la GRC sur le décès d'un membre actif à sa veuve, pour demander une pension.

Justice : communication de l'opinion d'un avocat sur le financement par le gouvernement canadien de l'Allan Memorial Institute. Le ministère a communiqué cette opinion (qui contenait des renseignements personnels sur trois hommes) après avoir obtenu l'accord des intéressés;

— communication de deux lettres à une étude juridique, pour documenter une plainte d'inconduite contre un avocat du ministère.

Secrétariat d'État : communication de renseignements sur la citoyenneté canadienne d'une femme, pour que les autorités japonaises puissent faire exécuter une ordonnance de garde à l'égard d'un enfant canadien.

— confirmation des dates auxquelles 13 personnes ont obtenu leur citoyenneté canadienne, pour déterminer leur qualification aux fins de l'Ordre du Canada. Trois dossiers n'ont pu être retracés.

Solliciteur général : communication à la Chambre des communes du rapport, issu des travaux de la Commission McDonald, qui recommandait comment le Canada devrait s'acquitter des obligations lui restant envers Warren Hart.

Statistique Canada : confirmation du lieu de naissance ou de l'âge de plusieurs personnes à des parents, pour qu'ils puissent réclamer les prestations de retraite ou pour confirmer la citoyenneté, afin d'établir des passeports canadiens ou américains;

— refus de communiquer des renseignements personnels sur des personnes nées dans les pays du bloc de l'Est et décédées au Canada sans testament.

Faites passer . . .

Le Commissaire à la protection de la vie privée et son personnel ont continué à parcourir le pays pour prêcher la bonne parole. Le Commissaire a notamment prononcé des allocutions devant les membres des clubs canadiens de Moose Jaw (Saskatchewan) et de London (Ontario). Il a parlé de vérification de la protection des renseignements personnels à l'Institut des vérificateurs internes; des cotes de protection à l'Association canadienne du marketing direct; de la protection de la vie privée et des droits de la personne au congrès de la Canadian Law and Society Association; de surveillance et de contrôle au congrès annuel des protecteurs de données internationales, à Québec; et — à la conférence nationale de gestion des dossiers à Melbourne, Australie — des incidences, sur la gestion de l'information, de la législation relative à la protection des renseignements personnels.

Comme la protection des renseignements personnels touche de près la collecte des statistiques (les statisticiens manipulent un grand nombre de dossiers administratifs), le Commissaire s'est adressé aux participants de la conférence des cadres de Statistique Canada et aux statisticiens internationaux, à Ottawa et à Stockholm. Il a donné en outre des entrevues aux médias et participé aux réunions de divers comités de rédaction de journaux.

Son personnel a fait des exposés au Centre de perfectionnement des cadres du gouvernement fédéral, et a pris la parole devant des classes de niveau postsecondaire, à des colloques de fonctionnaires fédéraux et aux réunions annuelles de l'Association canadienne de l'informatique et de l'Association canadienne des sciences de l'information.

Les demandes de renseignements

Le Commissariat a reçu cette année 1 248 demandes, allant du droit d'un bijoutier de demander à ses employés d'inspecter les sacs et les paquets de leurs collègues avant de quitter le travail, à l'appel d'une entreprise de service public qui aurait voulu utiliser les numéros d'assurance sociale pour retrouver les clients partis sans avoir payé leurs factures. Le cas de la bijouterie ne relève pas de la *Loi sur la protection des renseignements personnels* et l'entreprise de service public peut utiliser les NAS, mais la communication des numéros des clients ne lui donnera pas accès aux banques de données du gouvernement fédéral pour trouver les nouvelles adresses.

Un peu plus de 14 pour cent de demandes concernaient des demandes d'accès à des dossiers personnels, qui ont été renvoyées aux ministères qui détenaient les renseignements. Ce genre de requête révèle que beaucoup de personnes croient encore qu'Ottawa conserve un dossier épais à leur sujet — vision que le Commissaire est heureux de démentir.

Près de 50 pour cent des interlocuteurs ont posé des questions sur la *Loi*, demandé comment faire pour consulter les renseignements les concernant ou réclamé des précisions sur la *Loi*.

Environ six pour cent des demandes concernaient l'intrusion possible de programmes fédéraux dans la vie privée, comme les sondages de Statistique Canada et les nouvelles lignes directrices du gouvernement fédéral sur les conflits d'intérêt et les enquêtes de sécurité des fonctionnaires.

Dix pour cent des appels portaient sur la protection de la vie privée, mais n'étaient pas de compétence fédérale.

Le Commissariat peut maintenant renvoyer les Ontariens à leur nouveau commissaire à l'information et à la protection de la vie privée, quoique ce dernier ne puisse, lui non plus, régler les plaintes mettant en cause des entreprises du secteur privé.

Un certain nombre d'appels (un peu plus de sept pour cent) n'avaient rien à voir avec le Commissariat, telles des demandes d'indices permettant de retracer des parents naturels ou un appel pour savoir pourquoi un organisme de logement local réclamait la déclaration de revenus d'un requérant.

Les questions et les plaintes à propos d'incidents reliés au numéro d'assurance sociale ont augmenté (soit 15 pour cent des demandes), ce qui confirme en partie les propos qu'a tenus le Commissaire dans son dernier rapport, mais aussi parce que le gouvernement fédéral a promis de resserrer la collecte et l'utilisation des numéros dans ses propres services. Les plaignants se rebellaient de devoir fournir leur NAS pour voter lors d'élections municipales, pour faire partie d'un club de voyage de l'âge d'or et, dans un cas inusité, de voir leur NAS programmé dans la photocopieuse de l'employeur pour coder l'accès à l'appareil, en surveiller l'utilisation et les coûts.

La réceptionniste du Commissariat a renvoyé le nombre ahurissant de 5 756 appels au standard du gouvernement fédéral ou, plus récemment, à Référence Canada. La majorité de ces demandes étrangères à nos services s'expliquent par le numéro national sans frais fourni après l'inscription « Commissaire à l'information » (avec lequel le Commissaire à la protection de la vie privée partage ses bureaux) dans les pages bleues des annuaires téléphoniques municipaux. On prend le Commissariat pour le nouvel Information Canada.

Gestion intégrée

La gestion intégrée fournit des services en matière de finances, de personnel, de bureautique et de bibliothèque au Commissariat à l'information et au Commissariat à la protection de la vie privée.

Finances

Pour l'année financière 1987–1988, un budget de 3 922 000 $ et de 58 années-personnes fut alloué par le Parlement, ce qui signifie une augmentation d'approximativement 300 000 $ comparativement à l'exercice financier de 1986–1987. Les coûts en personnel furent de 2 970 000 $ et les frais de services professionnels et spéciaux, de 512 000 $. Ces montants représentent plus de 89 p. 100 des dépenses. Le reste du budget, soit 440 000 $, couvre tous les autres frais.

Finances
Voici l'état des dépenses des Commissariats pour la période du 1er avril 1987 au 31 mars 1988

	Information	Vie privée	Gestion intégrée	Total
Salaires	1968,062	1,121,001	483,768	2,572,831
Contributions aux régimes d'avantages sociaux des employés	159,200	149,640	88,160	397,000
Transports et communications	25,028	59,518	98,698	183,244
Information	47,258	50,028	558	97,844
Services professionnels et spéciaux	412,534	72,754	26,411	511,699
Location	76	727	11,172	11,975
Achat de services de réparation et d'entretien	222	1,163	1,225	2,610
Services publics, fournitures et approvisionnements	4,191	11,171	27,778	43,140
Construction, acquisition de machines et d'équipement	32,494	33,141	16,344	81,979
Autres dépenses	79	1,245	177	1,501
Total des dépenses	**1,649,144**	**1,500,388**	**754,291**	**3,903,823**

Personnel

Cinq employés ont été portés à l'effectif au cours de l'année financière, ce qui a fait passer l'effectif total à 58 personnes en date du 31 mars 1988. Il y a eu 21 opérations de dotation pendant l'année, dont une nomination à un poste de cadre de gestion, celui de Directeur général du Commissariat à la protection de la vie privée.

Administration

Nous avons, au cours de l'année écoulée, fait l'acquisition de locaux situés au 3e et au 4e étage de la tour B du complexe Place de Ville. Actuellement en voie d'aménagement, ces bureaux seront prêts pour l'été.

Bureautique

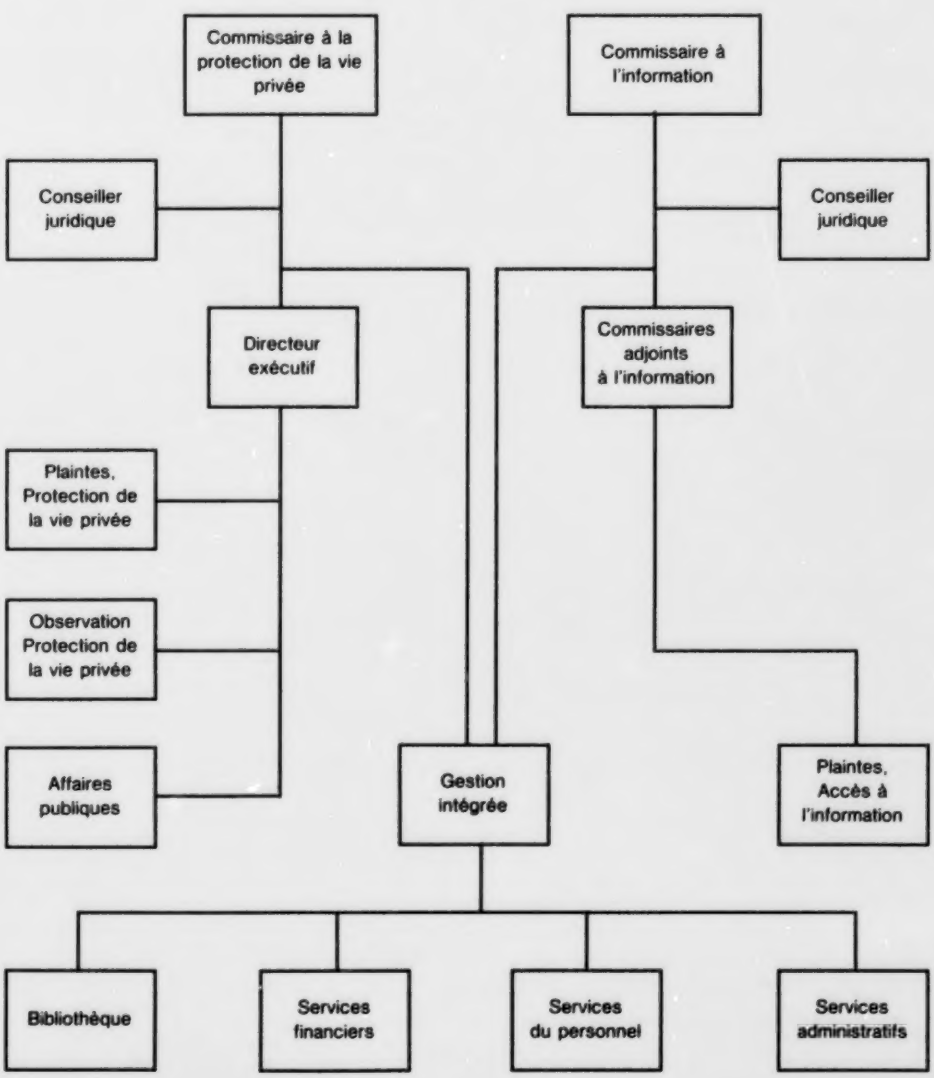
L'implantation de la bureautique s'est accentuée dans la plupart des secteurs, de sorte que le personnel maîtrise mieux cette technique. Une plus grande quantité d'information a été traitée et mise en mémoire.

Bibliothèque

La bibliothèque procède à des acquisitions et diffuse de l'information pour les deux Commissariats. À cette fin, les responsables de la bibliothèque souscrivent des abonnements à plusieurs bases de données bibliographiques et autres. Les usagers bénéficient également d'un service de prêts inter-bibliothèques. La liberté de l'information, la protection de la vie privée et la fonction de protecteur du citoyen sont les principaux centres d'intérêt de la collection, qui compte environ 3 000 ouvrages. Les personnes qui ont des ouvrages à consulter ou des travaux de recherche à effectuer sont d'ailleurs admises à la bibliothèque. L'an dernier, la bibliothèque a accueilli 25 visiteurs, répondu à 630 demandes de référence et acquis 450 ouvrages.

Annexe I

Commissariats
à l'information et à la protection
de la vie privée du Canada



Annexe II

Institutions fédérales assujetties à la Loi

Administrateur de l'Office du transport du grain

Administration de la voie maritime du Saint-Laurent

Administration de l'assistance à l'agriculture des Prairies

Administration de pilotage de l'Atlantique

Administration de pilotage des Grands Lacs, Limitée

Administration de pilotage des Laurentides

Administration de pilotage du Pacifique

Administration du pipe-line du Nord

Administration du rétablissement agricole des Prairies

Affaires des anciens combattants Canada

Affaires extérieures Canada

Affaires indiennes et du Nord Canada

Agence canadienne de développement international

Agence de surveillance du secteur pétrolier

Agriculture Canada

Approvisionnements et Services Canada

Archives nationales du Canada

Banque du Canada

Banque fédérale de développement

Bibliothèque nationale

Bourse fédérale d'hypothèques

Bureau canadien de la sécurité aérienne

Bureau de l'enquêteur correctionnel

Bureau de l'inspecteur général du service canadien du renseignement de sécurité

Bureau du Conseil privé

Bureau du contrôleur général

Bureau de la coordonnatrice de la situation de la femme

Bureau du Directeur général des élections

Bureau du directeur des enquêtes et recherches

Bureau du séquestre (biens ennemis)

Bureau de services juridiques des pensions

Bureau du Surintendant des institutions financières Canada

Bureau du vérificateur général

Centre canadien d'hygiène et de sécurité au travail

Centre d'information sur l'unité canadienne

Centre de recherche pour le développement international

Centre national des Arts, Corporation du

Comité externe d'examen de la Gendarmerie royale du Canada

Comité de surveillance des activités de renseignement de sécurité

Commissariat aux langues officielles

Commission des allocations aux anciens combattants

Commission d'appel de l'immigration

Commission d'appel des pensions

Commission canadienne des droits de la personne

Commission canadienne d'examen des exportations des biens culturels

Commission canadienne des grains

Commission canadienne du blé

Commission canadienne du lait

Commission de la Capitale nationale

Commission canadienne des pensions

Commission canadienne des transports

Commission des champs de bataille nationaux

Commission de contrôle de l'énergie atomique

Commission de l'emploi et de l'immigration du Canada

Commission d'énergie du Nord canadien

Commission de la Fonction publique

Commission d'indemnisation des marins marchands

Commission des lieux et monuments historiques du Canada

Commission nationale des libérations conditionnelles

Commission des plaintes du public contre la Gendarmerie royale du Canada

Commission de réforme du droit du Canada

Commission des relations de travail dans la Fonction publique

Commission de révision de l'impôt

Commission de révision des lois

Commission du système métrique

Commission du tarif

Commission du textile et du vêtement

Communications, Ministère des

Conseil des Arts du Canada

Conseil canadien des normes

Conseil canadien des relations de travail

Conseil consultatif des districts bilingues

Conseil consultatif de la situation de la femme

Conseil de développement de la région de l'Atlantique

Conseil économique du Canada

Conseil de fiducie du Fonds canadien de recherches de la Reine Élisabeth II sur les maladies de l'enfance

Conseil national de commercialisation des produits de ferme

Conseil national de l'esthétique industrielle

Conseil national de recherches du Canada

Conseil de la radiodiffusion et des télécommunications canadiennes

Conseil de recherches médicales

Conseil de recherches en sciences humaines

Conseil de recherches en sciences naturelles et en génie

Conseil de révision des pensions

Conseil des Sciences du Canada

Conseil des subventions au développement régional

Conseil du Trésor, Secrétariat du

Consommation et Corporations Canada

Construction de défense (1951) Limitée

Corporation commerciale canadienne

La Corporation du Pont international de la voie maritime, Ltée

Défense nationale

Département d'État au Développement social

Directeur de l'établissement de soldats

Directeur des terres destinées aux anciens combattants

Emploi et Immigration Canada

Énergie, Mines et Ressources Canada

Environnement Canada

Expansion industrielle régionale

Finances, Ministère des

Gendarmerie royale du Canada

Institut canadien pour la paix et la sécurité internationale

Investissement Canada (anciennement Agence d'examen de l'investissement étranger)

Justice Canada, Ministère de la

Monnaie royale canadienne

Musées nationaux du Canada

L'office Canada-Terre-Neuve des hydrocarbures extracôtiers

Office canadien du poisson salé

Office canadien des provendes

Office de commercialisation du poisson d'eau douce

Office des eaux des territoires du Nord-Ouest

Office des eaux du territoire du Yukon

Office des indemnisations pétrolières

Office national de l'énergie

Office national du film

Office des normes du gouvernement canadien

Office des prix des produits de la pêche

Office des produits agricoles

Office des recherches sur les pêcheries du Canada

Office de répartition des approvisionnements d'énergie

Office de stabilisation des prix agricoles

Pêches et Océans Canada

Les Ponts Jacques-Cartier et Champlain Incorporée

Revenu Canada

Santé et Bien-être social Canada

Secrétariat des relations fédérales-provinciales

Secrétariat d'État

Service canadien des pénitenciers

Service canadien du renseignement de sécurité

Service national des libérations conditionnelles

Sciences et technologie Canada

Société canadienne des brevets et d'exploitation Ltée

Société canadienne d'hypothèque et de logement

Société canadienne des ports

Société canadienne des postes

Société d'assurance-dépôt du Canada

Société de développement de l'industrie cinématographique canadienne

Société du crédit agricole

Société immobilière du Canada limitée

Société pour l'expansion des exportations

Solliciteur général Canada

Statistique Canada

Transports Canada

Travail Canada

Travaux publics Canada

Tribunal canadien des importations